THE BLACK REPORT 2018

DECODING THE MINDS OF HACKERS

nuix

LEAD AUTHOR
Chris Pogue

EDITOR
Josh Mehlman

DESIGN
Emilie Bertolino

DESIGN ASSISTANCE
Carina Custudio
Erin Decker
Val Nicol
Matt Schneider

PRODUCTION
Zehra Zaidi

PRODUCTION ASSISTANCE
Nichole Anderson
Matt Culbertson
Jessica Lyford
Rose Masidi
Andrew Nester
Rebecca Porte
Corey Tomlinson
Evan Tracy

WHAT'S INSIDE

05 CHAPTER 1: MAKING A DIFFERENCE

06 CHAPTER 2: PERCEPTION AND REALITY—THE TRUTH ABOUT HACKERS

08 CHAPTER 3: WHO ARE HACKERS?

12 Can Criminology Theory Explain the Motives of Hackers?
16 A "Safe and Secure" Environment
18 Year of the Mega-breach
20 Working with Nerds

22 CHAPTER 4: ATTACKS AND TARGETS

28 A Risk-based Approach to Penetration Testing Scope
30 What Security Experts Can Learn From First Responders
32 A Monster Inside of Me

34 CHAPTER 5: IN, OUT, GONE

36 In Asia, Cybersecurity Really Is the Wild West
38 Cyberthreat Intelligence: Make Sure It Means What You Think It Means

42 CHAPTER 6: SECURITY DEFENSES

46 There and Back Again: A Forensicator's Tale
48 Macro Viruses: Why Are They Still Even a Thing?
52 Strategies to Protect an Internet of Things

54 CHAPTER 7: WHAT HAPPENS AFTER AND WHAT DO YOU TELL THE BOARD?

60 The Convergence of Law and Cybersecurity
62 Security with Empathy: How to Deliver Security Findings and Not Be Hated
64 Is It Time to Rethink Authentication?

66 CHAPTER 8: APPENDIX—BREACH BREAKDOWN BY INDUSTRY

70 CHAPTER 9: THE FINAL WORD—OFFENSE IN DEPTH

01

WELCOME TO THE BLACK REPORT 2018

Last year we embarked on journey to write a cybersecurity report that was substantively different from all the others in the market: The Black Report. Our hope was that in being different, we could make a difference. In my humble opinion, we succeeded. The 2017 Black Report was downloaded, shared, printed, handed out, and ultimately read by more than 10,000 people! Not bad for our rookie year.

> *"Our hope was that in **being** different, we could **make** a difference. In my humble opinion, we succeeded."*

Before we begin the 2018 Black Report in earnest, it's important to understand who our respondents are. Last year, we focused on people who referred to themselves as hackers or professional penetration testers. This year, we broadened our survey to include incident responders. These guys deal first-hand with hackers and the aftermath of data breaches. And as you'll see, their perspective provided a tremendously valuable contribution to the results of the survey.

For clarity, we have defined a hacker as someone who accesses computer systems or applications without permission to execute nefarious activities for destruction or personal gain. Penetration testers are professional hackers who operate within the boundaries of a legal statement of work (commonly referred to as a get out of jail free card), that grants them permission to attack their target. It's important to note that this piece of paper is the primary difference between a malicious attacker and a skilled penetration tester, not the tools available to them or the techniques they use. Without this document, pentesters are engaging in criminal activity, so it's tremendously important.

We added incident responders this year so we could gain their insight into various types of current attacks, their opinion of organizational security posture, and the data types at risk. In questions that focused on hacking or motivation, either they didn't answer or we removed their responses from the sample.

We conducted this year's survey in much the same way as last year's with some new additions based on feedback from many of you. Respondents filled in the surveys anonymously online using Survey Monkey or in person during the week of Black Hat, Bsides Vegas, and DEFCON; affectionately known as hacker summer camp. Respondents who wanted absolute anonymity completed a paper survey during a Nuix event and turned it in to a staff member. Interestingly, more than half of our respondents used the paper option.

SO WHAT ELSE IS NEW?

I'm excited to tell you that our data sample is almost twice the size it was last year—112 respondents in total—and contains a much more widely dispersed geographic representation. Although nearly three-quarters of our respondents hailed from North America, we also surveyed people from Australia, Brazil, the Dominican Republic, Dubai, England, France, Germany, Ireland, Mexico, New Zealand, the Philippines, Singapore, and South Korea.

Most of them worked in North America (79%), however 26% worked in Europe, the Middle East, or Africa; 25% worked in the Asia Pacific region, and 16% worked in Latin America. Yes, I know that adds up to 146%, but it illustrates that many respondents work in more than one region. Some Nuix employees do business in all four of these regions, so it comes as no surprise to me that many of the respondents did as well.

We also added some questions about breaking the law, hacker motivation, and prior planning at the request of Dr. Thomas Holt of Michigan State University's Department of Criminal Justice, whom I collaborated with on improving some of the technical aspects of the survey. For the results of these questions, see Hacking and the Law on page 10.

Chris Pogue
Head of Services, Security and Partner Integration, Nuix

Chris has more than 15 years' experience and 2,000 breach investigations under his belt. Over his career, Chris has led multiple professional security services organizations and corporate security initiatives to investigate thousands of security breaches worldwide.

02

PERCEPTION AND REALITY: **THE TRUTH ABOUT HACKERS**

The cybersecurity industry has an annual cycle of reports that hit the streets sharing overviews and summaries of incidents the publishing organization—or its customers—experienced or engaged in since their last report. These reports provide a fascinating view into trends, often reporting on data culled and anonymized from actual incidents. These reports typically provide statistics such as window of intrusion, window of compromise, and dwell time. As well as observed trends from the past year, many reports also include projections of what the cybersecurity industry can likely expect in the future.

While the findings in these reports are interesting, each organization likely has a different client base, and hence a different data set from which they're operating. Some identify trends based predominantly on nation-state actors while others focus on the theft of credit card data.

WANT TO KNOW ABOUT CYBERATTACKS? ASK A HACKER

The Nuix Black Report takes a unique perspective. We have avoided using data acquired from incidents (which is often lacking due to a dearth of instrumentation and visibility within the breached environment) and interviewing cybersecurity leaders within their respective organizations (which has its own unique limitations). Instead, for the second year, Nuix sat down with professional hackers at Black Hat USA and DEFCON in Las Vegas, Nevada—the premier conferences for security professionals—and asked them to provide their observations and opinions.

The value of this approach goes beyond simply taking a different perspective. For example, information security professionals often recommend their clients develop and implement a computer security incident response plan (CSIRP) outlining the process and procedures they will use when responding to a security incident. A vital facet of developing that plan is determining which assets you're trying to protect: What are the "crown jewels" or critical value data (CVD) without which your organization could not continue to do business?

"Yet, whenever organizations sit down to develop their CSIRP, one person isn't at the table: the hacker. As such, the organization evaluates what data to protect and how to go about protecting it from the position of an insider or a business executive. Might it change things if you understood how someone would attack the organization or compromise its infrastructure?"

Yet, whenever organizations sit down to develop their CSIRP, one person isn't at the table: the hacker. As such, the organization evaluates what data to protect and how to go about protecting it from the position of an insider or a business executive. Might it change things if you understood how someone would attack the organization or compromise its infrastructure? Would it help to know you were protecting the right CVD, or perhaps more importantly, if your most vulnerable assets were data at all?

Looking back to the much-discussed Target breach, would anyone have expected the refrigeration contractor to work through a CSIRP development process and identify their connection to the retailer as a possible goal or success factor for an attacker? Would anyone have considered that perhaps Target's most vulnerable asset was not the data they had but to whom they were connected?

A PROBLEM OF TIMING: 300 DAYS VS 15 HOURS

This year's Black Report pays particular attention to how long it takes hackers to breach an organization, both by stages of the breach and by industry. The clear majority of respondents say they can breach most of their target organizations, locate critical value data, and exfiltrate that data within 15 hours.

Now compare the speed at which an attack can take place with how long it takes for the breached organization to find out about it. For example, Equifax discovered it was breached in July 2017 and the subsequent investigation found that the breach occurred earlier the same year. This is relatively fast; most industry reports say the average gap between a breach and its discovery is between 200 and 300 days.

Yes, it is true that many respondents to the Nuix Black Report are professional hackers or members of red teams who are contracted to breach organizations. And yes, those who hack in support of a contract operate under a different set of constraints to a dedicated threat adversary. For the most part, though, they observe many of the same goals and use the same techniques to achieve those goals. In fact, it's essential for penetration testers to do this to ensure they're giving customers the real-world testing necessary to assess their defensive posture.

It's also insightful to get an attacker's view of what constitutes "success" when breaching an organization. Understanding this perspective has a significant impact on how organizations should defend against and respond to security incidents and breaches to their IT infrastructure.

COMPARE YOUR ASSESSMENT

Perhaps the key takeaway from the Nuix Black Report is that your perception and understanding of the threat landscape may be in stark contrast to reality. The Black Report provides a much-needed and unique take on what attackers are targeting within breached organizations and how long it takes them to succeed, regardless of how the attacker determines success.

As you read through the findings, analysis, and opinions illustrated in this report, we highly recommend that you consider them in light of your own assessment of your organization's assets and how these findings affect your overall risk assessment.

Harlan Carvey
Director of Intelligence Integration, Nuix

Harlan has worked in information security for more than two decades. After serving on active duty with the United States military, he has worked across vulnerability assessments, digital forensics and incident response, and targeted threat hunting and response. Harlan is an accomplished public speaker and prolific author.

03

WHO ARE HACKERS?

As we did last year, we asked respondents a series of questions about their background and experience. Contrary to the popular idea of hackers, most went to university; 43% were college graduates and 32% had postgraduate degrees (no PhDs in our sample). Only 19% ended their formal education with a high school or general education development (GED) diploma, while 6% said formal education was for suckers (figure 1).

Respondents also held multiple security certifications. While the majority (60%) had less than three certifications, 22% had between three and five (incidentally, I fall into this group), 8% had six or seven, 5% had between eight and 10, and 5% held more than 10 technical certifications (figure 2).

Here we encounter an interesting paradox. Even though 40% of respondents held more than three technical certifications, a big majority (78%) did not believe these certifications were a good indicator of technical ability. So why take the time and expense of getting certified? Anecdotally they told us they believed certifications were necessary to secure employment, remain relevant, and advance their careers. However, they gauged technical acumen in more tangible ways such as how they performed on the job, how quickly they could learn new tasks, and how creatively they applied what they learned to their jobs.

Around one in five respondents (19%) have been hacking for between four and six years—while they're seasoned, they are still relatively new to the industry (figure 3). There were large groupings at the seven to 10-year range (16%) and veterans with more than 17 years of experience (15%). Only 10% had been hacking for between one and three years. This may be good news for organizations looking to hire experienced hackers but there is a worryingly low number of new people entering the industry.

Given the publicity about cybersecurity in the past few years, you might expect an influx of new people in the industry. However, one can't simply up and decide to become a pentester. While the tools required to become a hacker are easy to obtain (see Attack Types on page 24), becoming an effective pentester requires a deep understanding of many technical disciplines including web applications, networking protocols, programming languages, and server operating systems. It's hard to be a good pentester and it takes years to get up to speed.

The remaining respondents (21%) did not consider themselves hackers; these were more than likely the incident responders who filled in the survey this year.

Around a third of respondents (32%) worked for large enterprises of more than 50,000 people (figure 4). Another quarter were self-employed (9%) or worked at small consultancies (16%). Tied at 18% were small businesses from 20-499 people and medium-sized ones with 500-4,999 employees. The only safe conclusion we can draw from this is that hackers work for organizations of all sizes.

Our respondents one again showed that they took their craft seriously by spending considerable time bypassing IT security systems (figure 5). A third said they spent up to 10 hours each week actually hacking, while a combined 26% made a full-time duty of it, spending between 31 and 50 hours a week on the job. A workaholic 8% said they spent more than 50 hours a week p0wning.

1. WHAT IS YOUR HIGHEST LEVEL OF TRADITIONAL EDUCATION?

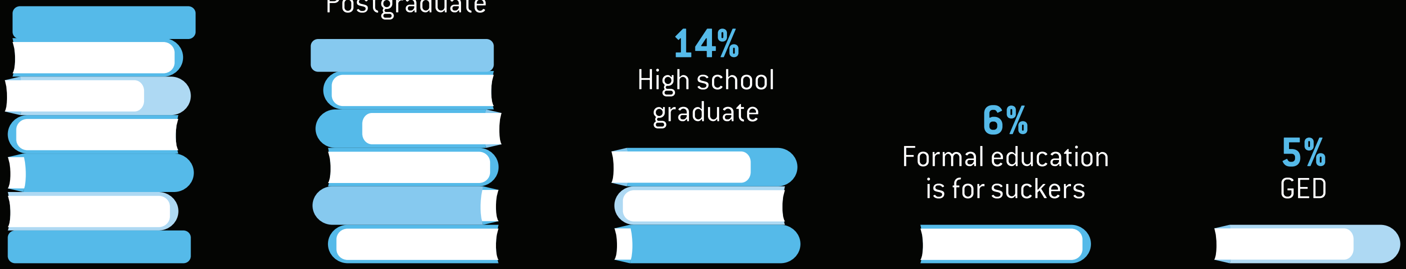
43% College graduate

32% Postgraduate

14% High school graduate

6% Formal education is for suckers

5% GED



2. HOW MANY TECHNICAL CERTIFICATIONS DO YOU HAVE?

<3	**60%**
3–5	**22%**
5–7	**8%**
7–10	**5%**
>10	**5%**

78% did *not* believe technical certifications were a good indicator of technical ability

3. HOW LONG HAVE YOU BEEN HACKING?

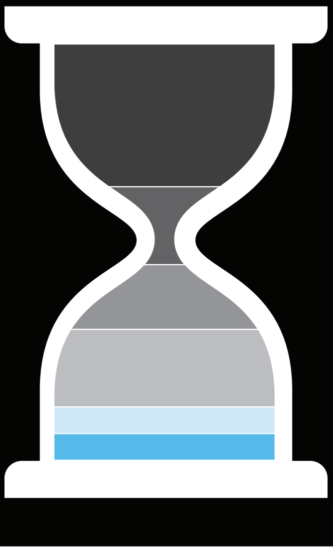
1–3 years	**10%**
4–6 years	**19%**
7–10 years	**16%**
11–13 years	**10%**
14–17 years	**9%**
17+ years	**15%**

34% have been hacking for more than 10 years

4. WHAT TYPE OF ORGANIZATION DO YOU WORK FOR?

Self-employed	**9%**
Small consultancy (less than 20 people)	**16%**
Small business (20–499)	**18%**
Medium sized business (500–4,999)	**18%**
Large business (5,000–9.999)	**3%**
Very large business (10,000–50,000)	**4%**
Enterprise (More than 50,000)	**32%**

5. HOW MANY HOURS A WEEK DO YOU SPEND BYPASSING IT SECURITY SYSTEMS?



● 0–10	**33%**
● 11–20	**18%**
● 21–30	**15%**
● 31–40	**18%**
● 41–50	**8%**
● >50	**8%**

HACKING AND THE LAW

We asked point blank, with the option not to answer, if respondents believed they had ever broken cybersecurity laws (figure 6). Surprisingly, 86% of respondents answered and 9% indicated that they had frequently broken cybersecurity laws. The majority (52%) indicated that they had sometimes broken laws, while 25% said they always stayed on the straight and narrow. It's worth mentioning again that the only difference between a law-breaking hacker and a sanctioned penetration tester is the legal terms laid out in a statement of work.

We also asked, optionally, if respondents had ever stolen company data when leaving an employer (figure 7). Just over one-third of our respondents (35%) admitted they had taken company data with them when they left, while 65% said they had not.

On the one hand, this is substantially lower than the figures frequently reported in security industry surveys such as the Ponemon Institute's, which are generally around the 60% mark. Maybe hackers don't need to take their employer's data because they can access it, or anyone else's data, whenever they want. Perhaps they already knew what was in their employer's data and decided it wasn't that valuable or worth the potential trouble. However, even if only one-third of an organization's employees take data that does not belong to them upon their departure, that is a substantial risk to any organization.

Further, the reason you hire a pentester is specifically to see if they can access your most critical data and systems. You want to be sure they're not going to make off with that data for nefarious purposes. This highlights the need to work with a reputable security service provider who values their professional reputation and to ensure your statements of work are detailed and specific. This may not prevent pentesters from accessing your data inappropriately, but it will provide a legal mechanism to address the issue after the fact.

In a similar vein, we asked our respondents if they had accessed their employer's critical value data (CVD) for personal gain; only 14% said they had (figure 8). Even so, those are disturbing numbers! For every 1,000 employees your organization has, 140 of them are accessing your CVD for their own purposes beyond that which their job requires. If this ratio held true across the nearly 7 million technology industry workers in the United States, just under a million of them inappropriately accessed company data.

Do you have your data hygiene and information governance in order? Maybe you should look into that.

WHY DO YOU HACK?

Next we asked some questions to understand a bit about the mindsets of attackers (figure 9). Almost all the hackers we surveyed were motivated by curiosity—86% said they liked the challenge and hacked to learn (respondents could choose more than one answer). One-third (35%) said they did it for the entertainment value or to make mischief ("the lulz"), 21% hacked for financial gain, and 6% said they hacked for social or political motives.

We asked hackers about their attitudes to risk and prior planning (figure 10). The most definitive results showed that 51% of respondents were planners, 64% were risk takers, 54% thought before they acted, 46% enjoyed some danger in their lives, and 37% didn't need self-control to stay out of trouble.

These questions may seem odd at first glance, but they tap into the criminological concept referred of self-control, or a person's ability to regulate their own actions.

People who plan, avoid risks, think ahead, and don't have to actively moderate their behavior are less likely to act on opportunities to engage in risky activities such as, say, downloading a client's data file or doing a little cross-site scripting on a vulnerable site.

As a caveat, having self-control doesn't mean you won't act, it just means you can better think through the impact of doing something risky or criminal. You may still take the chance if the opportunity seems too good to pass up. However, a person with low self-control would be more inclined to act immediately because they don't recognize the same impacts.

Based on these results, around two-thirds of respondents have moderate or strong self-control. The remaining third appear to struggle with self-control, which make it hard for them to restrain themselves when a clear opportunity arises.

Interestingly, there were correlations between the respondents who said they lacked self-control and those who:

- Admitted they had broken the law
- Reported taking data with them when they left a job
- Accessed an employer's data for personal gain.

The takeaway for me is that the hackers we surveyed were willing to take risks but often calculated ones that had an element of planning. Essentially, they aren't wild and reckless; they want to push boundaries but in a way they can do over and over again. They're not looking to BURN IT DOWN but if they can get away with it, they might make smaller cuts because they find it interesting and exciting.

6. HOW OFTEN DO YOU THINK YOU HAVE BROKEN CYBERSECURITY LAWS?

9% Frequently

52% Sometimes

25% Never

14% No answer

7. THIRTY-FIVE PERCENT

ADMITTED THEY HAVE TAKEN COMPANY DATA WITH THEM WHEN THEY LEFT A JOB

8. FOURTEEN PERCENT

ACCESSED AN EMPLOYER'S CRITICAL VALUE DATA (CVD) FOR PERSONAL GAIN

9. WHY DO YOU HACK?

(Respondents could select multiple answers)

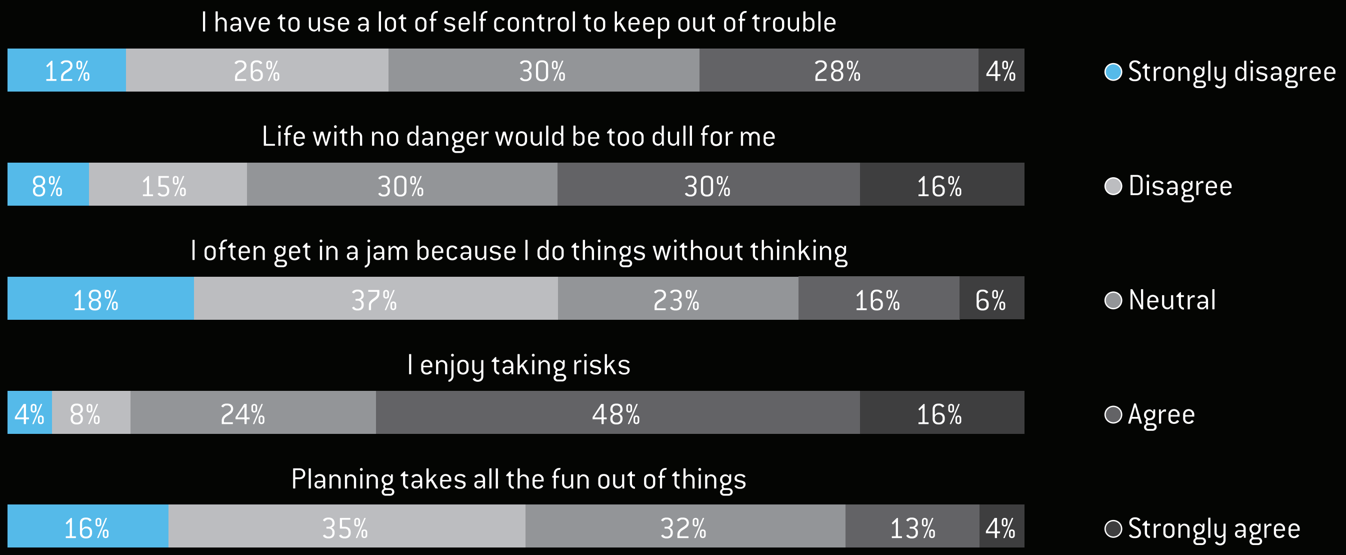
86% I like the challenge—I hack to learn

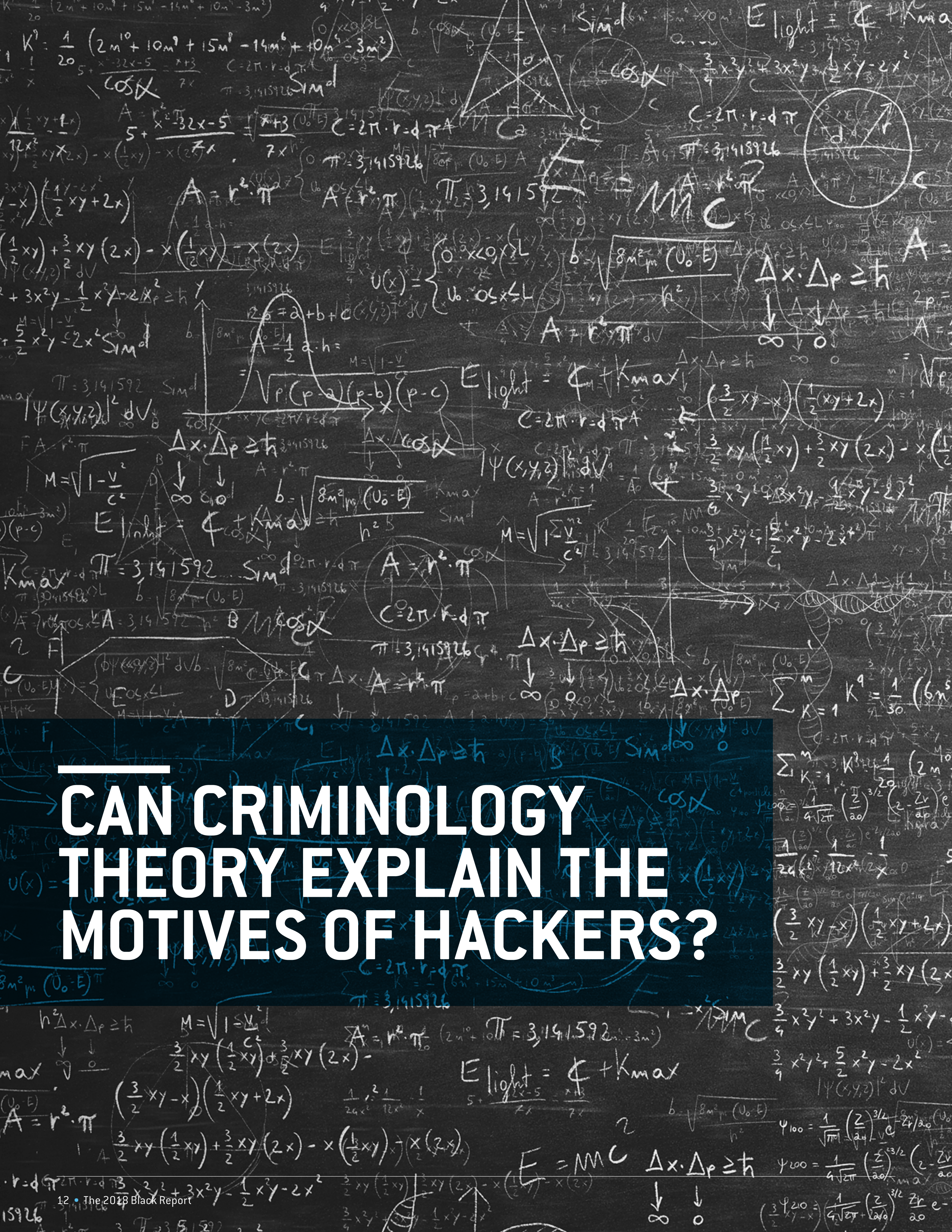
35% I hack for the lulz

21% I hack for financial gain

6% I hack for social or political moves

10. WHAT DO YOU THINK ABOUT RISK AND PLANNING?





CAN CRIMINOLOGY THEORY EXPLAIN THE MOTIVES OF HACKERS?

Over the past 100 years or more, social scientists have proposed many theories attempting to explain why people commit crimes.

Some of the earliest of these discussed whether crime was a conscious choice people engaged in after weighing the costs and benefits (classical theories) or a biological drive that offenders could not control (biological theories). Early psychological theories discussed the "criminal mind," including Freud's theories regarding the effect of disturbances at various stages of psychosexual development, and "weak consciences."

More recently, psychologists and criminologists looked to both personality and emotion as potential explanations for criminal behavior. They examined the effect of various characteristics on a person's ability to learn through punishment and rewards. Sociologists highlighted the importance of a person's socialization, social group, and culture for determining whether they defined crime and deviance positively and consequently engaged in it.

Many of these theories have changed or fallen out of favor. Contemporary evidence shows that no single theory explains every offender or every type of criminality. Instead, criminality seems to be created through bio-psycho-social influences—elements of a person's biology and psychology combine with culture and how they were socialized to promote or dissuade rule breaking. The power of the situation confronting a potential offender is also important; resource scarcity and interpersonal pressures are very real and strong influences. The resulting multi-pronged theories appear to have much more power in explaining many types of criminal offending and offenders.

WHY DO HACKERS HACK?

The literature available indicates that offenders engage in hacking knowing that it may be illegal and that some punishment might be involved should they be detected and caught.[1] However, hackers are not a homogeneous group and there may still be one of several different reasons or motives behind the behavior, including:

- Entertainment or curiosity
- Ego or intellectual challenge
- Entrance to social groups or status within them
- For a particular cause or because of malice
- Because of some justification such as security testing.[2,3,4]

Several criminology theories are available to explain the influences behind these motives.

RATIONAL CHOICE: THE BENEFITS OUTWEIGH THE COSTS

Rational choice theory states that people are rational actors who make individual decisions after carrying out a cost–benefit analysis.[5] In this case, crime is designed to meet a person's everyday needs of money, status, sex, and excitement.

Rational choice theories explain that, basically, if a person has the means necessary to commit a crime, if they desire the outcomes of such an act, and if the outcome outweighs the chance of getting caught and the punishment involved, then people will choose to commit the crime. In other words, the hacker might calculate that circumventing a particular security system is achievable, relatively risk free, and potentially lucrative financially, personally, or socially; thus they may decide to proceed.

This theory is helpful for explaining those motivated by money, entertainment, or social status where the risk of being caught and punished is overshadowed by the money, thrills, satisfaction, or kudos gained.

ROUTINE ACTIVITIES: CRIME OCCURS WHERE THERE IS OPPORTUNITY

Related to rational choice theory is routine activities theory.[6] This theory places more emphasis on the importance of the situation than the offender him- or herself; and states that crime will occur where there is a suitable target, a lack of capable guardians (security), and a motivated offender.

This theory highlights the importance of the opportunity to commit a crime. It posits simply that crime will occur when there is an opportunity; no diabolical super-predator is necessary. Routine activities theory is helpful in explaining hacking that is motivated by money, entertainment, intellectual challenge, or justifications.

STRAIN THEORIES: CRIME IS A REACTION TO NEGATIVE EMOTIONS

Although rational choice and routine activities theories are helpful for explaining crimes that people commit with some deliberation, other theorists have criticized their assumption that offenders make rational choices about their conduct. Strain theories, on the other hand, explain crime as being related to stress on an individual.[7,8] This stress creates negative emotions, which may motivate a person to respond in an effort to reduce these feelings. Crime is one response to this stress, which the offender may use to escape the strain, retaliate against the cause of the strain, or alleviate the negative emotions caused by the strain.

For example, a skilled computer engineer experiencing underemployment may use their experience to:

- Make money illegitimately, such as by stealing financial information
- Seek revenge on their employer by damaging their systems
- Engage in hacking in an effort to feel better by gaining status or satisfaction.

Strain theories are useful for explaining illegal hacking motivated by money, ego, status, or malice.

SOCIAL CONTROL: IT'S THE COMPANY YOU KEEP

Along with negative emotions, social bonds can also be very powerful motivators or deterrents for potential offenders. Hirschi's social control theory states that the strength of a person's bonds with conventional society—much more than the potential punishment if they are caught—dictate whether they are likely to violate laws.[9]

According to this theory, the extent to which a person is attached, involved, committed to, and believes in society's rules will raise or lower their chance of breaking them. Therefore, a potential hacker is more likely to break the rules if they:

- Are attached to others who do not conform to the rules or not attached to those who do conform
- Have spent relatively little time, effort and expense becoming ingrained in conventional society
- Are not involved with activities acceptable to most
- Do not believe in the norms and rules themselves.

> *"Criminological theories therefore have a lot to offer in terms of explaining the behavior of hackers. These theories are useful in determining the bio-psycho-social elements of these offenses, which can inform crime prevention strategies or at least provide a clearer understanding of the elements motivating these types of offenses."*

Most relevant to hacking behavior seems to be Hirschi's notions of attachment, commitment, and belief. So, if a hacker is strongly attached to other hackers, has little to jeopardize in terms of conventional status, and does not adhere to rules against hacking, they will be more likely to commit this type of offense. This theory is helpful for understanding hacking behavior motivated by status, cause, and justification.

FROM THEORY TO REALITY

To statistically test the motives of hackers, in 2017 Renushka Madarie examined a sample of 65 male hackers mostly from the Netherlands.[10] The responses of the hackers Madarie surveyed support several of these criminological theories to help explain hacking behavior.

The strongest motives self-reported by the hackers in this sample were intellectual challenge and curiosity. Correlational analyses revealed positive relationships between hacking and a need for peer-recognition or respect and team play. These results support the use of rational choice and routine activities theories, where opportunity, risk, and reward affect motivation.

On the other hand, the hackers surveyed in this sample also showed an aversion to values such as conformity, tradition, and security, reminiscent of Hirschi's description of a lack of beliefs in rules and norms. And similar to Hirschi's social control theory, the hackers in Madarie's sample were not indifferent towards these "conservation" values but rather their active disdain for them appeared to play a role in motivating their hacking activities. As the theory predicted, a lack of belief in traditional norms may lead to a failure of social bonds to prevent offending.

True empirical tests of how well theories explain hacking behavior are rare. Madarie's study indicates that criminological theories—which include biological, psychological, social, and cultural facets—may be helpful in describing the behavior of hackers. As evidenced in Madarie's work, theories including rational choice, routine activities, strain, and social control may explain the common motives of hackers, including thrill, recognition, and a lack of bonds to more traditional norms.

UNDERSTANDING THE ELEMENTS OF CYBERCRIME

Although hacking behavior is relatively new from a crime perspective, criminological theories have a lot to offer in terms of explaining the behavior of hackers. Although this behavior is relatively new from a crime perspective, these theories have been discussed and researched for many years, meaning many of them now rest on a strong, evidence-based foundation.

Criminological theories therefore have a lot to offer in terms of explaining the behavior of hackers. These theories are useful in determining the bio-psycho-social elements of these offenses, which can inform crime prevention strategies or at least provide a clearer understanding of the elements motivating these types of offenses.

[1] *Randall Young & Lixuan Zhang. Illegal Computer Hacking: An Assessment of Factors that Encourage and Deter the Behavior, Journal of Information Privacy and Security, 2007*

[2] *Australian Institute of Criminology, Hacking Motives, High Tech Crime Brief, no. 06, 2005*

[3] *Peter Grabosky & Russell Smith, Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities. Sydney: Federation Press, 1998*

[4] *Max Kilger, Ofir Arkin & Jeff Stutzman, "Profiling," in The Honeynet Project (ed), Know Your Enemy: Learning about Security Threats (2nd Edition), Boston: Addison Wesley, 2004*

[5] *Derek Cornish & Ronald Clarke. Understanding crime displacement: An application of rational choice theory. Criminology, 25(4), 1987*

[6] *Lawrence Cohen & Marcus Felson. Social change and crime rate trends: a routine activity approach. American Sociological Review, 44, 1979*

[7] *Robert Agnew. Foundation for a general strain theory of crime and delinquency. Criminology, 30(1), 1992*

[8] *Robert Merton, Social structure and anomie. American Sociological Review, 3, 1938*

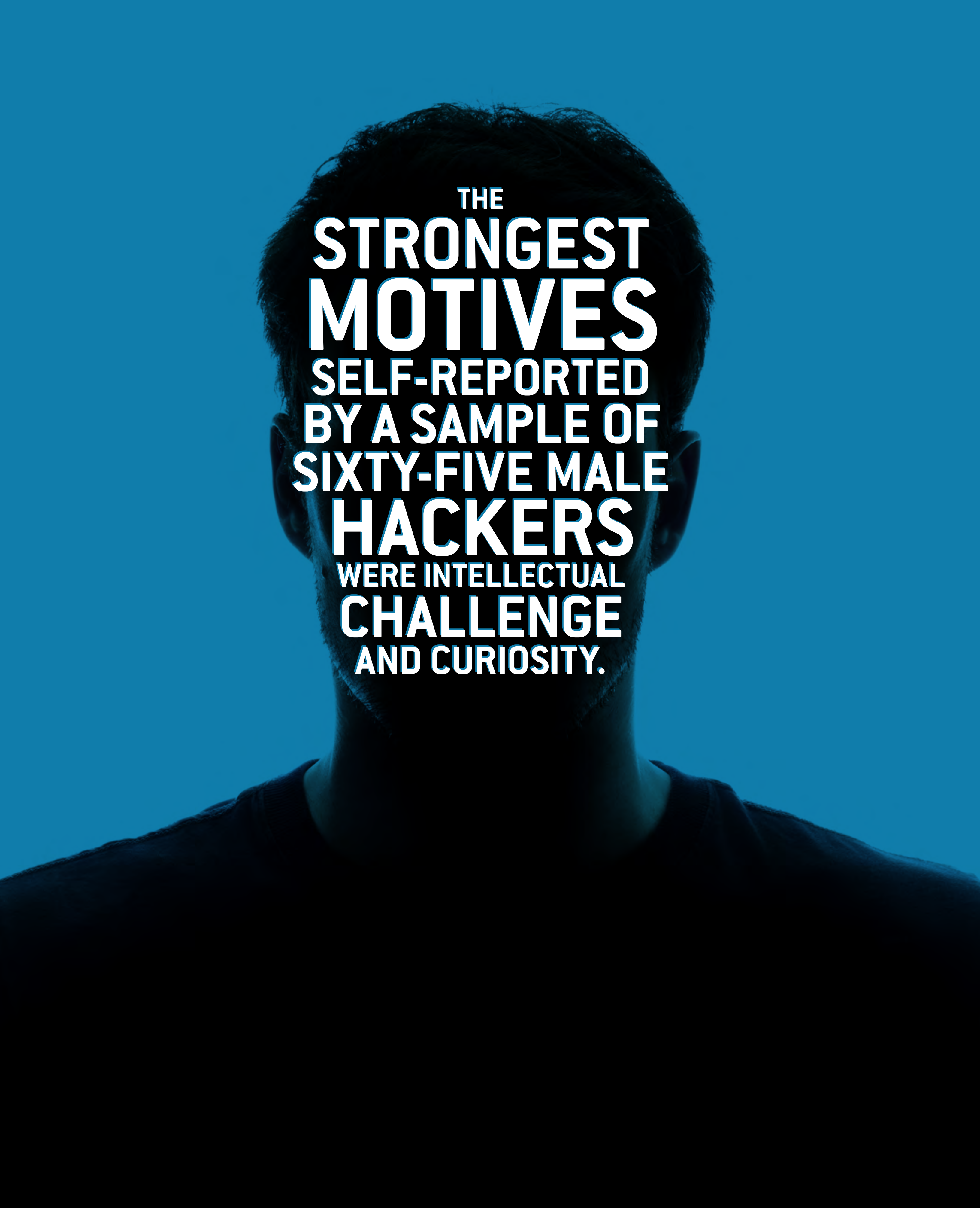
[9] *Travis Hirschi. Causes of Delinquency. Berkeley: University of California Press, 1969*

[10] *Renushka Madarie, Hackers' motivations: Testing Schwartz' theory of motivational types of values in a sample of hackers. International Journal of Cyber Criminology, 11(1), 2017*

Dr. Claire Ferguson

Senior Lecturer, Faculty of Law , Queensland University of Technology

Claire is a lecturer, researcher, and consultant in forensic criminology. Her main research areas surround offender evidence manipulation at homicide scenes, and equivocal death investigation. She offers training and expert consultancy to law enforcement agencies, as well as assistance to victims' families.



THE STRONGEST MOTIVES SELF-REPORTED BY A SAMPLE OF SIXTY-FIVE MALE HACKERS WERE INTELLECTUAL CHALLENGE AND CURIOSITY.

A "SAFE AND SECURE" ENVIRONMENT

The Australian Federal Police Cybercrime page opens with this statement: "A safe and secure online environment enhances trust and confidence and contributes to a stable and productive community." The statement itself is true, without a doubt. However, what we see happening in the world around us belies every word of it—our online environment is everything but "safe and secure."

The findings in the Nuix Black Report come from questions we asked security professionals who wear hats of varying shades. Their answers paint a picture that is equal parts educational and cautionary. How do those perspectives measure up, however, to the experience and teachings of some of the world's top law enforcement and investigative agencies? What lessons can we learn by examining the evidence with their experiences in mind?

LOWERING THE BAR, BROADENING THE FIELD

I started with the premise that organizations globally face more cybersecurity attacks now than ever before. We keep hearing this but what's behind it? Such a broad, steady increase can't have just one cause, can it?

Consider the following statistics:

- **More data, more problems**. According to Cisco, we generated 122 exabytes of internet protocol traffic each month in 2017. That number is forecast to grow to 278 exabytes in 2021. While figures like this are somewhat rubbery, there's no doubt our reliance on data will grow appreciably.
- **Continued attacks**. An article published by Entrepreneur magazine in November 2016 cited an average daily rate of 4,000 ransomware attacks, a 300% increase over 2015. Organizations of all sizes need to remain on constant lookout.
- **Broader attack surface**. In 2017 there were over 20 billion devices connected to the internet, according to Statista. These numbers are predicted to grow considerably, and also warrant a bit of skepticism.
- **Voracious appetite**. Worldwide, 5 billion pizzas are consumed annually. Roughly one-third of those are eaten by incident response teams.

OK, that last bullet is irrelevant and made up, although I stand by my assertion that IR teams make up their fair slice of that pie, pardon the pun. The other bullets are no surprise to anyone in the industry, or anyone who reads the news, but each constitutes a piece of the larger picture.

The deeper you look, though the more disturbing this picture becomes. According to the UK National Crime Agency, the "technical skill required to commit cyberattacks continues to decrease. Malware and services such as DDoS (distributed denial of service) are easily acquired on the dark web which means the number of individuals capable of launching basic cyberattacks is increasing.

"Anyone can be (or hire) a cybercriminal."

THE VIEW FROM THE INSIDE

There's a lot of debate about the difference between a "hacker" and an "insider threat." The U.S. Federal Bureau of Investigation brochure, The Insider Threat – An introduction to detecting and deterring an insider spy, claims "A company can often detect or control when an outsider (non-employee) tries to access company data either physically or electronically... However, the thief who is harder to detect and who could cause the most damage is the insider—the employee with legitimate access."

This is reflected in the Black Report; 35% of respondents claimed to have taken company data with them when they left a job and 14% acknowledged accessing their company's critical value data for personal gain. This is the classic definition of the insider, but there's another point of view.

"In my personal opinion, once the attacker is inside your firewall or network, once they're there, they're acting as an insider," said Bernard Wilson, a Network Intrusion Program Manager with the U.S. Secret Service, expressing his personal opinions based on years of experience in the field. "It's an east-west, lateral movement. If you can secure the network from an insider perspective, you'll deter the outsider as well. The most profitable approach to security is mitigating or minimizing the insider threat."

Taking Wilson's comments a step further, it doesn't make sense to define insiders narrowly as people who have legitimate access to your network and systems. Once hackers are inside your network and using stolen credentials, they're insiders. They're pretty much indistinguishable from your employees.

GO WHERE THE MONEY IS

When we step back to look at what criminals want to steal, the answer is simple: Personally identifiable information (PII). According to Wilson, it's as simple as Willie Sutton's (possibly apocryphal) explanation of why he robbed banks: "Because that's where the money is."

> *"Where we really need to be concerned is supply chain attacks. It's going to be more and more a major form of attack that doesn't get enough press. Many attackers are using this to gain access to secured systems."*

The FBI dedicated a two-part series to the topic in June 2017—Building a Digital Defense Against PII Theft. The agency noted a significant increase in reports of this kind of theft over the years. PII theft is the centerpiece of virtually every data breach, whether it's achieved by impersonating someone the victim trusts, blindly phishing a group of targets, or some other attack.

"The majority of the investigations that I've been involved with from a federal perspective—1028 fraud with ID docs, 1029 access device fraud, 1030 fraud in connection with computers—involved PII; It's an ongoing problem and an area of concern," said Wilson.

If you believe in the "follow the money" perspective, some of the more interesting targets are ruled out because hackers can't effectively monetize them. These include automobiles, healthcare devices like pacemakers, and airplane entertainment systems.

One target stood out to Wilson in our conversation. "Where we really need to be concerned is supply chain attacks," he said. "It's going to be more and more a major form of attack that doesn't get enough press. Many attackers are using this to gain access to secured systems."

A familiar example is the attack on Target, where hackers compromised a third-party air conditioning system vendor rather than attacking Target's systems directly. These attacks are more dangerous because the targeted systems or processes might not be under the control or supervision of the larger, better equipped company.

"If I can't get to the company directly, I can attack something that's maybe not sound or protected, but that I know they're going to use," Wilson concluded.

A WORLD WITHOUT PRIVACY

All told, government agencies' perspectives on security aren't much different from what we already know. Perhaps that's the most frustrating element for the industry: The dialog doesn't change overly much, we know there's a problem, and yet it persists.

Organizations that hold valuable data face an uphill battle. They must constantly defend from a position of weakness. Attackers have the advantage of surprise and defenders never know for certain exactly when, or how, a given attack will come. All we know is that the attack is inevitable.

For individuals, it means something else entirely. Privacy is a central concern in many countries. The European Union, Australia, and Japan have all adopted regulations dedicated to protecting their citizens' privacy and making it compulsory to notify them if their data is breached. Should that even be the goal? Or is privacy in the traditional sense dead?

"The reality is, we live in the information age and that means, if there's something that I want to obtain bad enough, I'll eventually be able to," said Wilson. "But can I leverage the information that I've captured? We talk about two-factor authentication and tokenization—it's not good enough that I have your credit card number, it has to be in a usable format.

"We're beyond privacy, but what do we do now? From a security perspective, we have to accept that fact, and turn our focus to that reality."

It remains to be seen if organizations of all shades—private, and public—can take that advice and create meaningful, effective defenses that correspond with an environment where they are constantly under siege, at a disadvantage, and likely to be vilified if they fail at an impossible task.

When you look at it that way, the promise of a "safe and secure online environment" feels like a fairytale.

Corey Tomlinson

Content Manager

Corey helps manage Nuix's content marketing efforts including the Unstructured blog, Unscripted podcast, case studies, and white papers. He has over 10 years' experience in marketing communications. He helped build a large financial institution's counter-insider threat program, developed cybersecurity awareness and education programs, and worked as a technical training instructor and curriculum designer.

THE YEAR OF THE MEGA-BREACH

The past 12 months have been filled with stories of companies being hacked and losing millions of records. Does this mean the bad guys are sitting on piles of stolen identities and credit card numbers? Are they wondering how to turn those digits into cash?

In short, no.

Typically, most ecommerce and point-of-sale system breaches are smash and grabs. The perps know they have a limited time before those stolen card numbers show up as being associated with fraud and are worthless. It's not uncommon for a company to be breached and the same day seeing those credit card numbers for sale on the dark web.

Fresh credit card numbers are typically priced anywhere between US$5 and $30 per number. Your identity? Unfortunately that's almost worthless, averaging about US$1.50 per Social Security Number record. With these low prices, just how much are the bad guys walking away with from a breach?

Take a look at some of the large breaches from the past 12 months and see the attacker's potential profits in the chart below.

New breaches are disclosed every day and it's easy to understand why. Attackers always go where the money is, and the criminal underground can make hundreds of millions of dollars off of stolen identities and credit cards. With the poor state of cybersecurity at most organizations, this trend will continue for years to come.

Chris Brewer

Cybersecurity Consultant, Incident Response, Nuix

Chris has more than 16 years' professional IT experience, including five years dedicated to information security. He has investigated many data breaches involving state-sponsored attacks and zero-day exploits. Chris has also worked as a systems administrator and a security analyst.

ORGANIZATION	BREACH	DATA LOST	REVENUE
WASHINGTON STATE UNIVERSITY	An attacker broke into a locked security cabinet, which contained a hard drive the school administration used to back up student records and other systems	1 million records including Social Security Numbers, names, addresses and health information	1 million Social Security Numbers at $1.50 per record, $1.5 million
SONIC DRIVE-IN	Credit card stealing malware installed on several point of sale systems, potentially exposing millions of credit and debit cards	Nearly 5 million credit card records	5 million fresh credit card numbers at a minimum of $5 each, at least $25 million
COPILOT PROVIDER SUPPORT SERVICES	An attacker accessed a poorly secured database on the Copilot website and obtained patient records	220,000 patient records including Social Security Numbers	220,000 Social Security Numbers at $1.50 per record, $330,000
EQUIFAX	An attacker took advantage of a known vulnerability in Apache Struts to compromise the web server and then move into the network	200,000 credit card numbers, 149 million identities	200,000 credit cards at $5 each, $1 million; 149 million Social Security Numbers at $1.50 each, $223.5 million

TOP 6 BREACHES OF 2017

EQUIFAX

VERIZON

UBER

RNC CONTRACTOR

INTERCONTINENTAL HOTELS GROUP

CHIPOTLE

Source: https://www.checkmarx.com/2017/12/31/recap-biggest-data-breaches-2017/, https://www.identityforce.com/blog/2017-data-breaches

WORKING WITH NERDS

Every company has them. You can usually find them in the IT department or tech support. Their discussions include words that sound a tad inappropriate for the workplace, such as “dongle” and “massage the metadata.” The last time they wore a suit was at a wedding or funeral—and they looked totally awkward in it.

But then a couple of years ago, I landed a job with a company that had a large number of technical people. (My IT expertise started and ended with Microsoft Office and Google.) Now I work with nerds.

Working with very technical individuals was very intimidating; I worried I wouldn’t be able to keep up. Today I can confirm that some rumors about working with nerds are true, some are completely false, and others are probably just a phishing email trying to get you to click.

THEY NEED TO KEEP LEARNING

One of the first things I noticed about working with nerds was the importance they placed on learning and improving their skills. They’re not always the best at taking vacations, working regular hours, or taking a break from a project before it’s done. If I’m awake at 3am, I can always count on at least one person being awake and on our Skype channel. They make their own hours and their own rules. They make sure they complete whatever is set before them. Whether they’re studying for a technical certification, proving a theory about Game of Thrones, or working a penetration test for a client, the concept of “working hours” doesn’t compute.

THEY COULD HACK MY LIFE BUT ARE HOPELESS WITH MICROSOFT WORD

My background is in education so if you ask me how email gets from one person to another? Not sure. How did this malware get into my laptop? No clue. How can I tell if someone has been on my system? You’re hilarious. But I know my way around Microsoft Office.

The people I work with are the opposite. They do a great job but they need my help making PowerPoints look nice, creating images and flow charts, making sure their documents are readable, and recently, removing a hyperlink from a Word document.

THEY’RE SMART BUT THEY CAN BE JERKS

Most nerds are fairly well rounded. They tend to be dedicated to hobbies outside of cybersecurity. On my team we have a guy who brews his own beers, an avid hunter, one who collects really nice watches, and one who loves everything Disney. These same people can penetrate companies’ environments, figure out weaknesses in their systems, send phishing emails out to test employees’ training, and detect where other criminals have attacked in the past.

One important thing I have had to remember is that the nerds I work with don’t have a filter. They say what they want. Usually they don’t intend to hurt other people’s feelings, they just want to get the facts out. More than once, I’ve had to shrug off a rude response to a question about something they knew that I didn’t.

THE HOODIE STOCK PHOTO IS KINDA TRUE

Spending time with my team, it’s clear their wardrobe choices have a similar theme: dark. I’m not sure if it’s for the slimming factor, or maybe it’s the nature of their work? The usual choice, no matter what event we were at, included a dark shirt, jeans, and a backpack. This could be cocktail attire, meeting attire, or a nice dinner. Fashion is not at the top of their requirements. I am usually the person who stands out in their crowd.

IN SHORT: DIFFICULT BUT REWARDING

Being a part of this team is a constant learning experience for me. They challenge me to do research, they nag me to be safe in my online practices, and they’re always looking for ways to give me a hard time.

I wouldn’t say they are just like everyone else, because they aren’t. They’re better. They continually learn and adapt to new environments, they ask for help when they need it, and they don’t bother with mundane things.

Working with nerds can be difficult on many levels but I know they’d be the first to help if I clicked that ad link!

Anonymous

ATTACKS AND TARGETS

One of the most widely quoted findings from the 2017 Black Report was the time it took for an attacker to breach an organization's perimeter. In case you forgot (or don't have last year's report handy), 71% of respondents last year claimed they could breach a target in less than 12 hours. This year we decided to extrapolate by further breaking it down into stages of a breach and the industry of the target. We've summarized the results here but you can see the full breakdown by stage and industry in Appendix A: Breach Breakdown by Industry on page 66.

Across all industries, 71% of respondents believed they could breach the perimeter of a target within 10 hours (figure 1). In the hospitality and food and beverage industries, 18% of respondents claimed they could breach a target in less than an hour and all of them said they could achieve that objective within 15 hours.

Next we asked respondents how long it took them on average to identify critical value data (CVD) once they had gained access to the target environment. Our results show that once they have breached the perimeter, attackers can move laterally with ease to map out the target environment and find what they are looking for.

Averaged across all industries, most respondents (54%) could find their target data within five hours. Large numbers could find the data they sought in less than an hour in the hospitals and healthcare (38%), hospitality (33%), and retail (30%) industries.

This illustrates the reality of "candy bar security," where an organization's security posture is crunchy on the outside and chewy in the middle. It's the result of focusing on hardening the perimeter of a network and assuming that anyone who's on the inside should be there and is doing what they're supposed to be doing. These assumptions are clearly not realistic today, if they ever were.

Once a pentester has breached the perimeter and identified CVD, the final task is to copy the data from a system controlled by the victim to a system controlled by the attacker (exfiltration). This was no challenge at all for most respondents.

Averaged across all industries, 40% of respondents could exfiltrate data in less than an hour and an additional 33% could do so within five hours. Our respondents saw the hospitals and healthcare, sports and entertainment, retail, and hospitality industries as particularly soft targets.

WHICH INDUSTRIES HAVE THE WORST SECURITY?

In reviewing this data we can draw several conclusions. First, the industries that presented the easiest targets for our respondents to compromise, identify CVD, and exfiltrate that data were:

- Food and beverage
- Hospitality
- Retail (figure 2).

A majority of respondents, or very close to it, said they could breach organizations in these industries—from initial compromise to data exfiltration—in less than 10 hours, with statistically relevant percentages claiming they could complete the entire process in less than five hours.

Another four industries had below-average results, indicating they were easier than most to target:

- Hospitals and healthcare providers
- Law firms
- Manufacturers
- Sports and entertainment companies.

It's interesting to point out that most of these industries are subject, in the United States, to cybersecurity regulations that specify which defensive countermeasures they should deploy. Industries that rely on high volumes of credit card transactions—such as retail, hospitality, and food and beverage—must comply with the Payment Card Industry Data Security Standard (PCI DSS). Healthcare providers must also comply with the Health Insurance Portability and Accountability Act Health Information Technology for Economic and Clinical Health (HIPAA HITECH).

Our data makes it clear that these compliance regimes do not guarantee that a regulated entity is meeting the prescribed requirements or that the regulations are having the intended impact. I've said it before but it's worth repeating: Compliance does not equal security.

While the legal industry has no specific regulations, the American Bar Association (ABA)'s Commission on Ethics 20/20 Report to the House of Delegates notes that the amendment to Model Rule 1.6(c) is intended to clarify that "a lawyer has an ethical duty to take reasonable measures to protect a client's confidential information from inadvertent or unauthorized disclosures as well as from unauthorized access."

According to the Report, unintended disclosure may happen when information is:

- Inadvertently disclosed, such as when an email is sent to the wrong person
- Accessed without authority, such as when a third party hacks into a law firm's network or a lawyer's email account
- Released without authority, such as when an employee posts confidential information on the internet.

Rule 1.6(c) makes clear that lawyers are ethically obligated to make reasonable efforts to prevent these types of disclosures, such as by using reasonably available administrative, technical, and physical safeguards.

Weak guidance, inconvenience, a lack of legal compulsion, and ignorance all undoubtedly contribute to the apparent lack of cybersecurity at law firms. I am not sure, though, why these factors or a combination of them do not outweigh the potential impact of a breach. The Panama Papers incident showed the world what happens when a firm's sensitive information is exposed. Skyrocketing costs of expert consultants, the potential for protracted litigation, the threat of government inquiry, and the inevitable loss of customer confidence and market share paint a portrait of devastation. You would think this is the call to action the industry has been waiting for.

ATTACK TYPES

We asked respondents what kinds of attacks were their favorite to execute (figure 3). More than a quarter said they favored network-based attacks (28%) closely followed by social engineering (27%) and phishing attacks (22%). (Yes, I understand that phishing is a form of social engineering but considering how prevalent they are today, I wanted to break them down individually).

Our respondents use a variety of software tools during attacks (figure 4). Based on the feedback we received, hackers most frequently used open source tools followed by exploit packs. When combined, more than 80% of respondents said they used these two types of tools, which is not surprising since they are easily available at no cost and very often do the job. The least used tools were private exploits, custom (handmade) tools, and commercial tools.

The interesting aspect of these results is that there is essentially no threshold to obtain the tools necessary to launch an attack. Anyone, anywhere with the skills and the desire can obtain what they need to become a hacker at low or no cost. (It does, however, take time and effort. See Who Are Hackers? on page 8.)

In contrast, most effective security defense technologies are expensive and difficult to deploy, manage and monitor. Once again, it seems that the advantage goes to the attackers.

Even if social engineering isn't the entire attack, hackers often use these techniques during the reconnaissance phase to get information such as names, job titles, usernames, passwords, and the configuration of systems they're trying to break into. In fact, only 12% of respondents said they never used social engineering to obtain information about a target (figure 5).

Of the respondents who used social engineering, 62% favored phishing, while 22% preferred getting down and dirty with physical attacks, and 16% got on the phone (figure 6).

This underscores the findings from the previous Black Report as well as this year's, that security training for employees at every level of the organization is a vital part of a holistic defensive strategy. Security is everyone's responsibility; the sooner you can get the entire organization involved, the better!

STAYING CURRENT

We're constantly hearing that organizations face a dynamic threat landscape with attack techniques constantly evolving to work around current defenses. If attackers are constantly changing, we can't rely on static defenses to keep them out—our security needs to be adaptive.

To get an idea of how dynamic this landscape was, we asked hackers how often they changed their attack strategies (figure 7). Nearly a quarter (22%) were complacent, sticking with the same techniques for a year or more. We can logically conclude that either these guys aren't very good at their jobs or there is no need to change; their attacks are working and if it ain't broke, don't fix it. The same proportion of respondents switched things up every couple of months. Slightly smaller numbers changed their attack methodologies at least twice a year (20%) or at least once a year (19%). The smallest percentage (17%) said they changed attacks with every engagement.

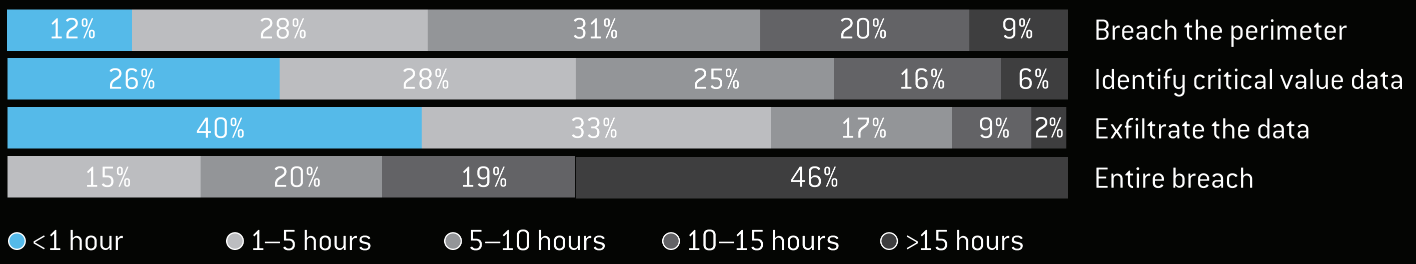
We also wanted to know if the release of new tools or techniques enabled our attackers to be better hackers (figure 8). More than one-third (37%) said they find something to make them better every month or two. Just under a third (29%) found something new in in every engagement (eek... these are the guys and gals to really watch out for!).

Cybersecurity is a broad field with many areas of complexity so it's not surprising that everyone occasionally needs to go somewhere for help or advice. Our survey showed that hackers most often used forums and IRC (internet relay chat) sites to get information on the latest techniques, closely followed by independent researchers and social media (figure 9). They were less trusting of security vendor blogs and websites, which is a shame because we have a lot of useful things to say! Coming in dead last was news sources. This is understandable since news organizations tend to report on what already happened rather than provide technical support or advice (although a hacker version of Dear Abby would be pretty funny).

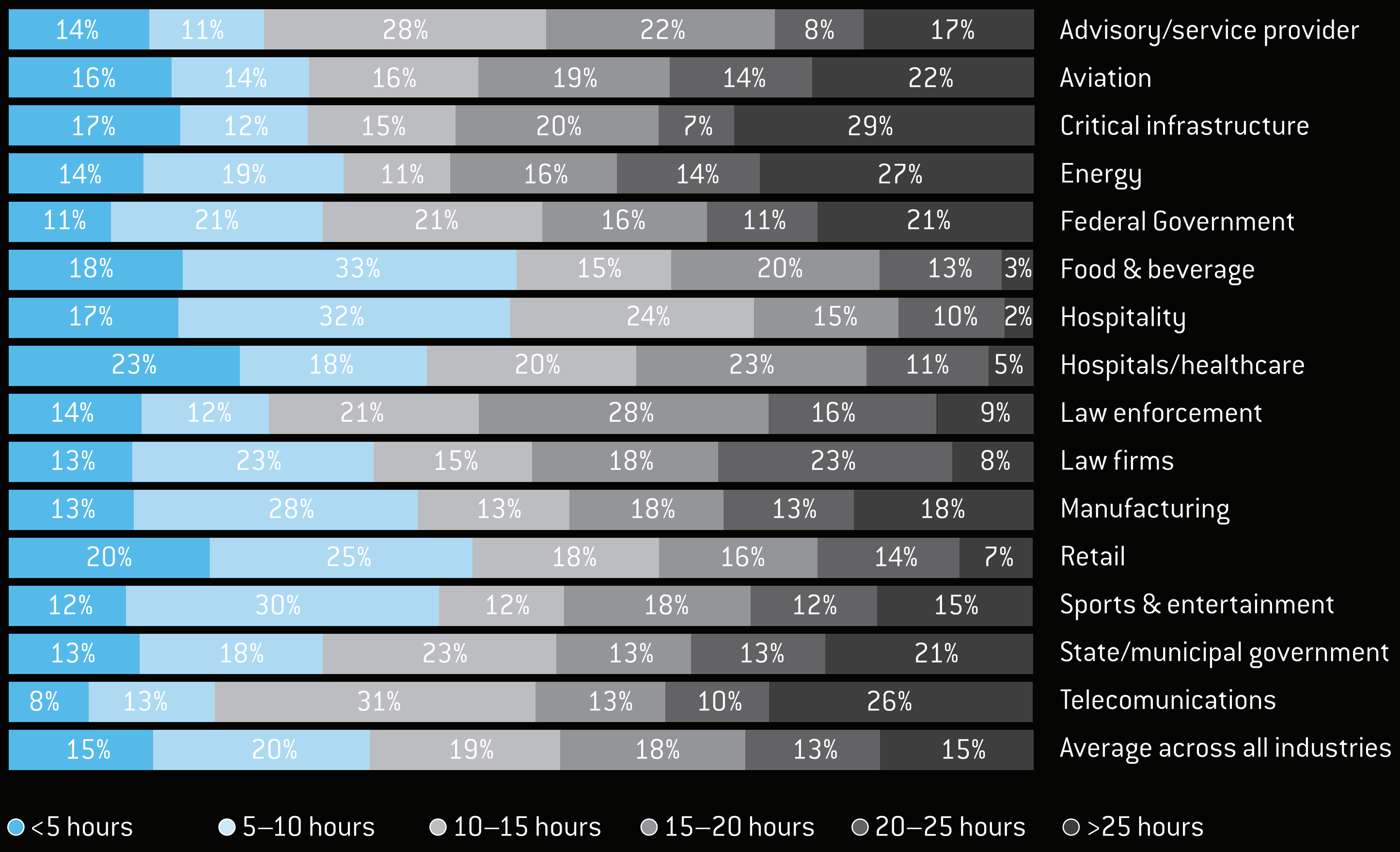
Almost half of our respondents (48%) spend between one and five hours a week keeping up with the latest news, trends, and technologies (figure 10). The remaining half spend six, 10, or more hours each week reading and researching while a negligible proportion didn't devote much time at all.

If cybersecurity is an arms race and knowledge is a weapon, are security specialists and incident responders spending as much time researching how to get better at their craft? Based on the data in this report, specifically the time it takes to compromise a target and how rarely our respondents were detected, it seems likely they are not.

1. HOW LONG DOES IT TAKE TO BREACH THE PERIMETER, IDENTIFY CRITICAL VALUE DATA, AND EXFILTRATE THAT DATA?



2. HOW LONG DOES IT TAKE TO BREACH THE PERIMETER, IDENTIFY CRITICAL VALUE DATA, AND EXFILTRATE THAT DATA (COMBINED)?



3. WHAT IS YOUR FAVORITE TYPE OF ATTACK TO EXECUTE?

Ransomware
3%

Waterhole
7%

Physical
13%

Phishing
22%

Social engineering
27%

Network attacks
28%

4. WHICH TOOLS DO YOU USE MOST FREQUENTLY?

Open source tools
4.02

Exploit packs
3.17

Custom tools you write yourself
2.74

Commercial tools
2.69

Private exploits
2.35

Average score for each option, higher scores = more frequently used

5. HOW OFTEN DO YOU USE SOCIAL ENGINEERING TO OBTAIN INFORMATION ABOUT A TARGET?

Always
17%

Often
33%

Sometimes
38%

Never
12%

6. WHAT IS YOUR FAVORITE TYPE OF SOCIAL ENGINEERING ATTACK?

16%
Phone

22%
Physical

62%
Phishing

7. HOW OFTEN DO YOU FIND YOUR ATTACK METHODOLOGIES ARE OUT OF DATE OR EASY TO DETECT?

Every engagement	17%
1–2 months	22%
2–6 months	20%
6–12 months	19%
>12 months	22%

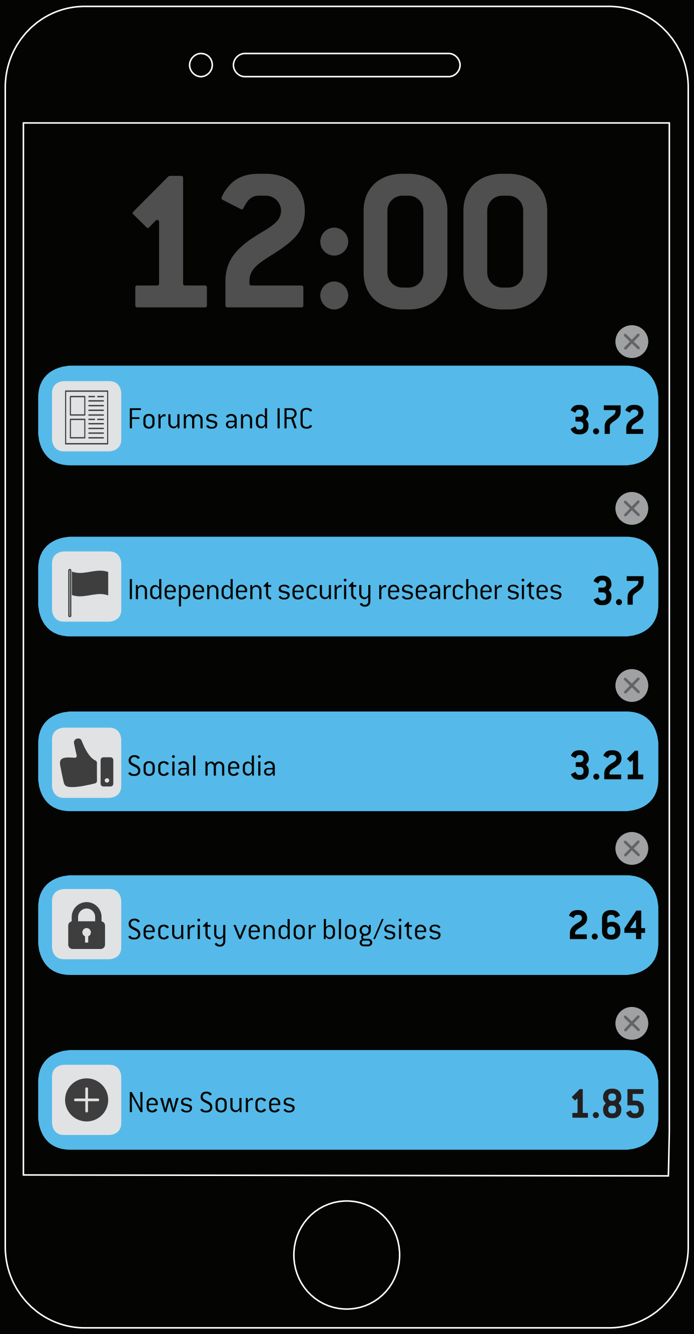
8. HOW OFTEN ARE NEW TOOLS OR TECHNIQUES RELEASED THAT ENABLE YOU TO ATTACK MORE EFFICIENTLY?

Every engagement	29%
1–2 months	37%
2–6 months	20%
6–12 months	10%
>12 months	4%

10. HOW MUCH TIME PER WEEK DO YOU SPEND KEEPING UP WITH SECURITY NEWS, TRENDS, AND TECHNOLOGIES?

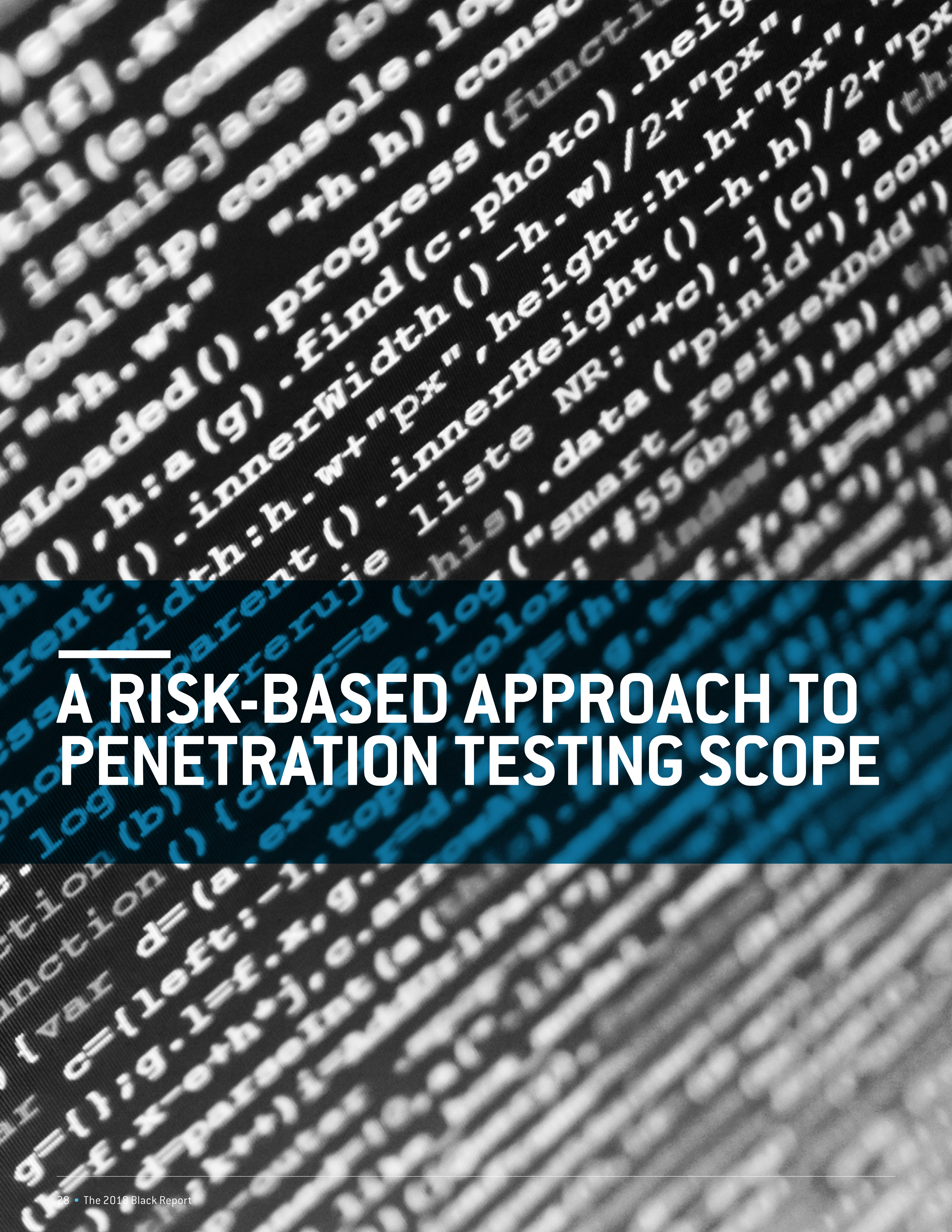
<1 Hour	2%
1–5 hours	48%
6–10 hours	34%
>10 hours	16%

9. WHERE DO YOU GO FOR INFORMATION ABOUT SOCIAL ENGINEERING OR EXPLOITATION TECHNIQUES?



Forums and IRC	3.72
Independent security researcher sites	3.7
Social media	3.21
Security vendor blog/sites	2.64
News Sources	1.85

Average score for each option, higher scores = more frequently used



A RISK-BASED APPROACH TO PENETRATION TESTING SCOPE

You'd never think an air conditioning system or an aquarium could lead to a data breach. However, these are exactly the kinds of assumptions people make when they're scoping penetration testing engagements—and this is to their peril.

Defining scope is the most important yet most overlooked part of a penetration test. Two big attacks I have worked on come to mind. At Target, it's now well known that threat actors used a vulnerable air conditioning system to gain access to customer data; and a casino was recently breached through the systems that ran a smart fish tank.

These two attacks had quite uncommon points of entry. If you had to guess, would you say these organizations had penetration tests scoped to include everything on the network or just those systems the client believed were a major concern?

Which made me wonder, what is going on when organizations score their pentesting engagements? Can there be a better way?

WHAT KIND OF PENETRATION TESTS DO ORGANIZATIONS CONDUCT?

Figure 1 is from Rapid7's white paper "Under the Hoodie: Actionable Research From Penetration Testing Engagements". It best illustrates the gap between external and internal tests completed and these statistics reflect the majority of tests I've conducted.

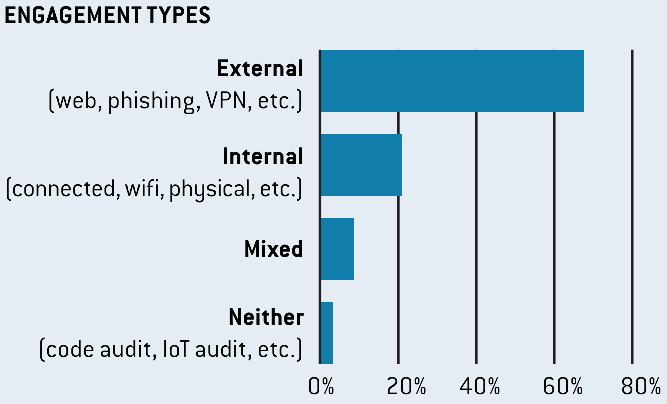


Figure 1: Types of penetration testing engagements. Source: Rapid7

Rapid7's research found the vast majority of engagements included externally facing assets. Most often, organizations are concerned with the systems that are easily reachable by a wide audience, and for good reason. Externally facing systems are subject to regular hostile scans by threat actors using a variety of tools, including Shodan. Because of this, they are understandably a top priority for organizations.

However, externally facing servers are not the only way into your network and the precious data it contains. There may be other risks you haven't considered.

SECURITY-DRIVEN SCOPE

Clients can purchase a variety of different types of testing. Typically during the sales call to initiate testing, we simply ask the customer what they'd like tested. Sometimes the client may have business needs such as PCI compliance and sometimes they just want to keep on top of issues. This brings in another question: How can we better explain scoping and better assess the right scope for clients?

In an ideal situation, instead of asking customers what scope they have in mind, we should ask questions about the network and then figure out the best scope together. As a security professional, I am not always part of the sales experience but I often have clients who come to me with questions about the scope during the first process of the engagement. This is the right point for security professionals to come into the process, ask the client questions about their environment, and assess how they can close the gap between assessing the easily accessible targets and providing a risk-based approach to scoping without drastically increasing the price of the engagement.

A risk-based approach starts with systems that contain high-risk data and then moves on to systems with data that has a lesser classification. This approach can provide many organizations with an easy answer to scoping that doesn't break the budget.

Ashley Knowles

Cybersecurity Consultant, Penetration Testing, Nuix

Ashley has more than seven years' experience in the information technology industry with four years dedicated to information security. She has managed hundreds of highly technical penetration tests and red team engagements, simulating advanced threat actor attacks on network and web applications.

WHAT SECURITY EXPERTS CAN LEARN FROM FIRST RESPONDERS

A data breach may not be a life-or-death situation—although that's plausible if it's a medical device company, a hospital, or a home security system and in the worst cases a breach could spell the death of a company. However, like emergency first responders, security professionals are often the first ones on the scene once a breach has been identified and need to start bringing order to a chaotic situation. This led me to wonder what security professionals can learn from these first responders.

TRAINING

To keep their skills sharp and stay abreast of the latest techniques and tools available, first responders train regularly. Security professionals also need to keep their skills sharp, follow the latest attack vectors, and bone up on the latest security tools.

The challenge in the security world is that most training is self-learned, such as by reading online forums. In fact, most of the hackers we spoke to in the Black Report were skeptical of formal training avenues such as certifications. However, you run the risk of learning incorrectly. Mentors have become increasingly popular in information security and for the most part people are willing to answer questions. The challenge is formalizing that process.

COMMUNICATION

First responders are always communicating. The dispatcher communicates with the caller and the services, the services communicate with each other and those in need. There is constant talk. This is a necessary and important part of emergency response. As someone who has a chronic illness and has been in the hospital more times than I care to admit, I have learned that the non-verbal and tone aspects of communication are just as important as the words.

These behaviors aren't innate; they're something first responders learn. You can learn them too.

In the security world, communication is often a problem. Communication between a client and a security professional can be challenging. Very few security professionals know how to speak the language of business to communicate the risks of security threats or the benefits of security controls. Many security professionals oversell the impact of potential threats. While miscommunication is rarely intentional or malicious—because it's hard to be accurate when the threat landscape changes as rapidly as it does—it makes things harder for everyone involved.

KNOW THE LAW

First responders know what they're allowed to do and what they're not. If they have to cross a line, they understand where the line is and soberly assess the risks. They can make snap decisions because they've had years of training and apprenticeships.

Security professionals also need this knowledge and ability to make informed decisions. Those who perform vulnerability exercises must understand the scope of the contracts they are engaging in and how these contracts protect them from legal action. If you're doing incident response and digital forensics, you must understand evidence handling and chain of custody laws, as well as your disclosure and communication responsibilities. You must also be aware of any industry-specific legal obligations (such as the Health Insurance Portability and Accountability Act and the Payment Card Industry Data Security Standard) as well as relevant laws for data privacy and breach disclosure.

FILTER OUT THE NOISE

When arriving at the scene, a first responder only knows what the dispatcher could find out from the caller who reported the emergency. They must immediately assess the situation, filter out the irrelevant noise, and identify the key elements relevant to the job at hand. To do this, first responders follow set procedures. They stick with these processes no matter how much those involved would like them to handle things differently.

Security personnel called in during an incident response must also follow a set response procedure to help limit the exposure of the breach and handle the digital evidence appropriately. Clients often push security professionals to do things outside their scope of work or to get to the end goal first. You may need to explain the importance of getting the client's business up and running as quickly as possible to minimize costs.

STAY CALM

First responders know how to stay calm no matter how much noise, yelling, or panic is going on. They rely on instinct and training to get people through the situation without showing any panic they may feel themselves. This keeps their heads clear.

Security professionals need to do the same. Whether you're scoping the security requirements for systems, performing a security assessment, or responding to an incident, be calm. There will be pushback. The customer will challenge the recommendations. There will be distractions. Whatever happens, try to speak to the client calmly and empathetically.

Evan Oslick

Software Security Consultant, Nuix

Evan conducts research and creates proofs of concept to secure the technology used by Nuix. He also manages a software security incident response team and performs web application penetration tests for customers. Before joining Nuix in 2015, Evan worked in application security for 11 years and spent 10 years as a software engineer.

A MONSTER INSIDE OF ME

It seems like almost every day there's a new story about a data breach and they keep getting worse and worse. Why are they happening? A common thread I have found is that a lot of attackers come in through a vector that no-one is really talking about: third-party access.

> *"The logic for attackers is obvious. Why struggle to defeat large organizations'defenses when you can attack their vendors much more easily? In addition, if you compromise one popular vendor, you might have access to hundreds or thousands of other organizations. An attacker can sit in the third-party network for years and continually breach its customers."*

THE PARTNER IS THE PROBLEM

I've investigated data breaches in complex and well-managed networks and in simple networks with little or no controls. More and more I see that the weak point is a compromised vendor or partner—the attackers are already in the vendor's network and come in through a network bridge, a virtual private network (VPN), or a remote access system such as Logmein.

The logic for attackers is obvious. Why struggle to defeat large organizations' defenses when you can attack their vendors much more easily? In addition, if you compromise one popular vendor, you might have access to hundreds or thousands of other organizations. An attacker can sit in the third-party network for years and continually breach its customers.

Typically, as I've done these investigations I've found that third-party access was the vector and the third party will have very high-level access to an organization's infrastructure. This is usually because the third party has dictated how it will operate and support its customer and this requires having local admin or domain admin rights. On the other hand, the vendor has very few responsibilities, and is not required to share with its customer if it gets compromised.

Third-party access is one of the most dangerous risks any organization can take on. You have to trust that your supplier's network defenses are strong enough to detect an attacker in its network.

WHERE DO WE GO FROM HERE?

Based on my experience, the only safe way to proceed is to assume your vendor will be compromised (if it hasn't been already) and has limited ability to detect or remediate the breach. Assume the vendor doesn't have your organization's interests on their radar so that's your job. This includes:

- Auditing third-party access to your systems more than any other user for credential sharing, unauthorized logins, account usage, and more
- Putting in place tight policies and controls on the third-party access and usage.

In an ideal world, if it emerged that the third party was the vector of a cyberattack, it would disclose this to its customer(s) or to the public rather than sweep it under the rug. Not talking about it, the current approach, will not solve the problem and will see it getting worse and worse.

Ivan Iverson

Senior Information Security Consultant, Nuix

Ivan conducts forensic analysis and provides threat hunting services for Nuix customers. He is a digital forensics and incident response subject matter expert with 17 years' experience in information security. Before joining Nuix, Ivan conducted incident response for Home Depot and digital forensics for the FBI.

05

IN, OUT, GONE

As we saw in the previous section, most respondents said they could complete an entire data breach in less than 15 hours, while significant numbers said they could break into some industries in less than five hours.

Cybersecurity survey after survey has shown that data breaches remain undetected for hundreds of days (averages remain around 200–250). Many organizations are very clearly ill-equipped to mount any sort of meaningful defense against their adversaries. Factors like diverse security tools, lack of realistic training and threat simulations, and dramatic price differences between hacking tools (mostly free) and enterprise security tools (mostly more than a BMW) are without question exacerbating the imbalance between attacker and defender.

Strong evidence of this imbalance was that 77% of respondents said they were identified by their targets less than 15% of the time (figure 1). Six out of seven times, attackers break into their targets, gather and exfiltrate the data without getting caught. These are not good odds. You would likely not play these odds in Vegas, yet huge percentages of organizations play them with their critical value data.

> *“Six out of seven times, attackers break into their targets, gather and exfiltrate the data without getting caught. These are not good odds. You would likely not play these odds in Vegas, yet huge percentages of organizations play them with their critical value data.”*

Another interesting data point we identified was that 74% of respondents did not believe that security professionals had a good understanding of what they were looking for when trying to identify attacks (figure 2).

FOOTPRINTS IN THE SNOW

Because the hackers we surveyed so rarely got caught out, we were interested to know if they ever took the time to cover their tracks (figure 3). Surprisingly (at least to me), 70% told us they took some sort of action to throw would-be responders off their trail.

That said, most respondents don’t put a lot of effort into obfuscation (figure 4). The largest percentage (31%) said it took them around 10 minutes, while 13% said it was trivial, taking them less than a minute, and 15% only spending around five minutes to cover their tracks.

Overall, almost three-quarters of respondents say they can cover their tracks after a breach in less than 30 minutes. This could (and likely does) add significantly more complexity to detecting their activities after the fact, depending on the attack type and what sort of obfuscation they used. It’s not clear if this is part of the reason why most organizations struggle with detection but certainly stands to reason. However, for organizations that conduct detection and response training, it seems wise to add the obfuscation aspect of an attack to their curriculum if they have any hope of identifying these thorough adversaries.

1. ONCE YOU'VE COMPROMISED A TARGET, HOW OFTEN DOES YOUR CLIENT'S SECURITY TEAM IDENTIFY YOUR PRESENCE?

Always (100%)
3%

More often than not (50–90%)
2%

Less than half the time (15–50%)
18%

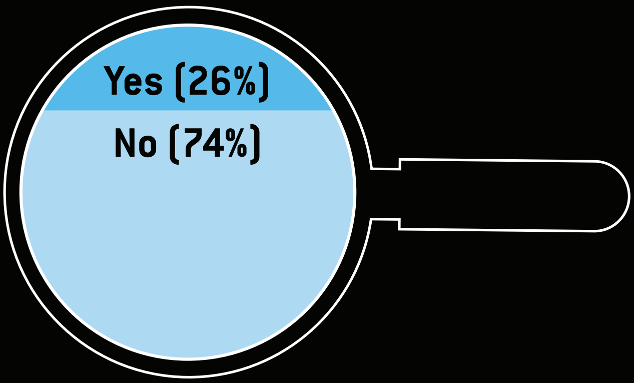
Rarely (5–15%)
75%

Never
2%

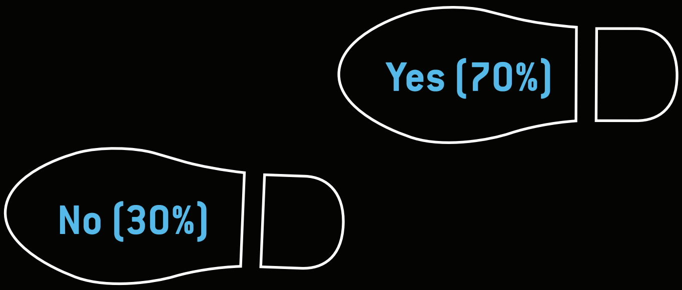
77%

SEVENTY-SEVEN PERCENT
SAID THEY WERE IDENTIFIED BY THEIR TARGETS LESS THAN FIFTEEN PERCENT OF THE TIME

2. DO YOU THINK MOST SECURITY PROFESSIONALS TASKED WITH DETECTING ATTACKS UNDERSTAND WHAT THEY'RE LOOKING FOR?



3. HAVE YOU EVER USED A TOOL TO COVER YOUR TRACKS?



4. HOW LONG DOES IT TAKE TO OBFUSCATE ATTRIBUTION?

More than an hour
7%

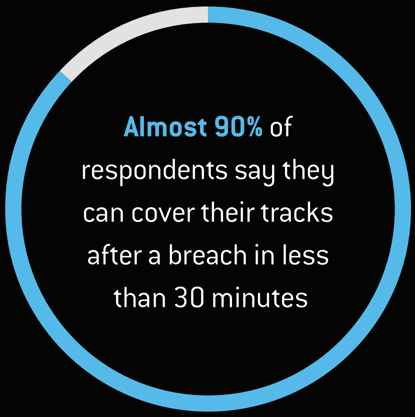
30–60 minutes
6%

15–30 minutes
28%

5–10 minutes
31%

1–5 minutes
15%

Less than a minute
13%



Almost 90% of respondents say they can cover their tracks after a breach in less than 30 minutes

IN ASIA, CYBERSECURITY REALLY IS THE WILD WEST

Asia is an up-and-coming hotbed of cybersecurity awareness. Major attacks are regularly reported in the news, consumers are asking developers about the security of their apps, and regulations will soon take effect in several core regional markets.

The question "What is the current state of security in Asia?" has a simple answer, but one that requires a bit of explanation on how security awareness evolves within a community.

I believe security matures within a community over four phases: perimeter defense, attribution as a deterrent, defense in depth, and monetization and insurance.

> *"One of the challenging factors of cybersecurity is the speed at which the problem emerged and how quickly it continues to develop. Cybersecurity evolves in a constant tension between offensive and defensive technologies."*

1. PERIMETER DEFENSE

Stories from the American Wild West are perfect for describing this phenomenon. When settlers first moved west, they uprooted their families, their belongings, and everything they knew. They brought along their valuables, currency, and other items to use for barter. After they settled in an area, the community would erect a bank or central storehouse as a place to facilitate trade.

The walls of this storehouse are the equivalent of traditional perimeter defenses for cybersecurity. The doors to the rickety wooden building acted as surrogate firewalls. Sometimes the entryways were guarded by dudes with guns and these sentries acted as an unmonitored intrusion prevention system.

We all know how the rest of the story goes: Jesse James rounds up a posse, brings an overwhelming force to storm the doors to the bank, and steals all the money. The vulnerability here is a predictable defensive force; all Jesse James needs to do is bring more dudes with guns than the bank has as protection.

It is a similar problem in cybersecurity; an adversary finds a vulnerability on an open port, crafts an exploit for the network application, and before too long steals the data. The adversary can probably even reuse that exploit on several other victims before the security industry finds a solution.

After the bank robberies, the community reacts with outrage. They realize that predictable perimeter defenses and the lack of effective response capabilities lead to successful attacks. This is when the transition to phase two begins, when the community starts spending more effort on identifying and catching the bad guys. In cybersecurity, we call this "attribution."

2. ATTRIBUTION AS A DETERRENT

Now the community has established that perimeter defense is an ineffective security strategy, it starts to build new organizations, tools, and processes for identifying bad guys. The Wild West's answer to outlaws was the Pinkerton National Detective Agency. The agency's job was to find out everything it could about Jesse James, catch him, and prevent bank robberies by letting other bad guys know they would also get caught.

We know how this worked out too; Pinkerton was exorbitantly expensive (sound familiar?) but even after Jesse James was brought to justice, bank robberies kept happening. In fact, the whole saga romanticized the profession of robbing banks, leading to a sharp increase of similar crimes, not to mention a century of novels, movies, and comics.

Similarly, the net effect of attribution campaigns is that it becomes cool to carry out cybercrimes. It's another ineffective prevention strategy, and the community knows it. Deterrents may work to some degree but often have an adverse effect during this phase of security evolution. Attribution is very expensive and no matter what you try, bad guys are still going to steal your money.

3. DEFENSE IN DEPTH

This is where things really start getting interesting. Organizations within and across sectors establish communication channels. They create processes for mitigating risk and the community shifts towards response-based security strategies.

Modern banks have thick walls, security glass, and guards as preventive measures. The placement of security countermeasures in a bank branch makes it clear they are maximizing the response capability rather than trying to prevent robberies altogether—because that's impossible.

Thick walls funnel would-be robbers through specific entryways; cameras are mostly pointed inward; tellers have emergency buttons they can press; and banks hire off-duty police officers and trained security specialists as guards.

Walls aren't as effective at preventing crime as you may believe; even if they're thick, the bad guys can still back tow-trucks through them. Cameras record the activity for later review and to enable investigation (response). Tellers' emergency buttons are linked to police dispatch centers so local authorities can send trained personnel to subdue the bad guys (response). Security guards are more useful as trained observers who can provide credible witness statements for criminal prosecution and insurance claims (also response).

None of these countermeasures will prevent all bank robberies. However, in combination and over a long enough period, banks can collect enough evidence to begin predictive analytics. The community learns which building designs limit the number of robberies and how much an average robbery will cost. Banks share this data with law enforcement to help lock up bad guys, with other banks to help them with their security strategies, and with insurers.

4. MONETIZATION AND INSURANCE

The last phase, and the hardest to achieve as a community, is monetization. It normally requires a high degree of coordination between governments, industry, and community to work effectively. You need to collect a lot of data to find the right predictive model.

Once this happens and insurance can affordably and predictably assume the risks of attack, the community has achieved security maturity.

WHERE ARE WE UP TO?

The United States, as a whole, is somewhere in the middle of phase 3 for cybersecurity. We can predict or prevent some attacks but we don't have enough data to make cybersecurity a viable business for insurers.

One of the challenging factors of cybersecurity is the speed at which the problem emerged and how quickly it continues to develop. Cybersecurity evolves in a constant tension between offensive and defensive technologies.

This means some sectors, such as the payment card industry, are getting close to phase 4. Others, such as power companies, are at the earlier stages of the defense in depth phase.

In Asia, where I live and work, even the more mature markets are mostly in some part of phase 1. The emerging markets are largely cash-based societies, which means the cybersecurity problems they face are unique to their region. I'd say they're pre phase 1.

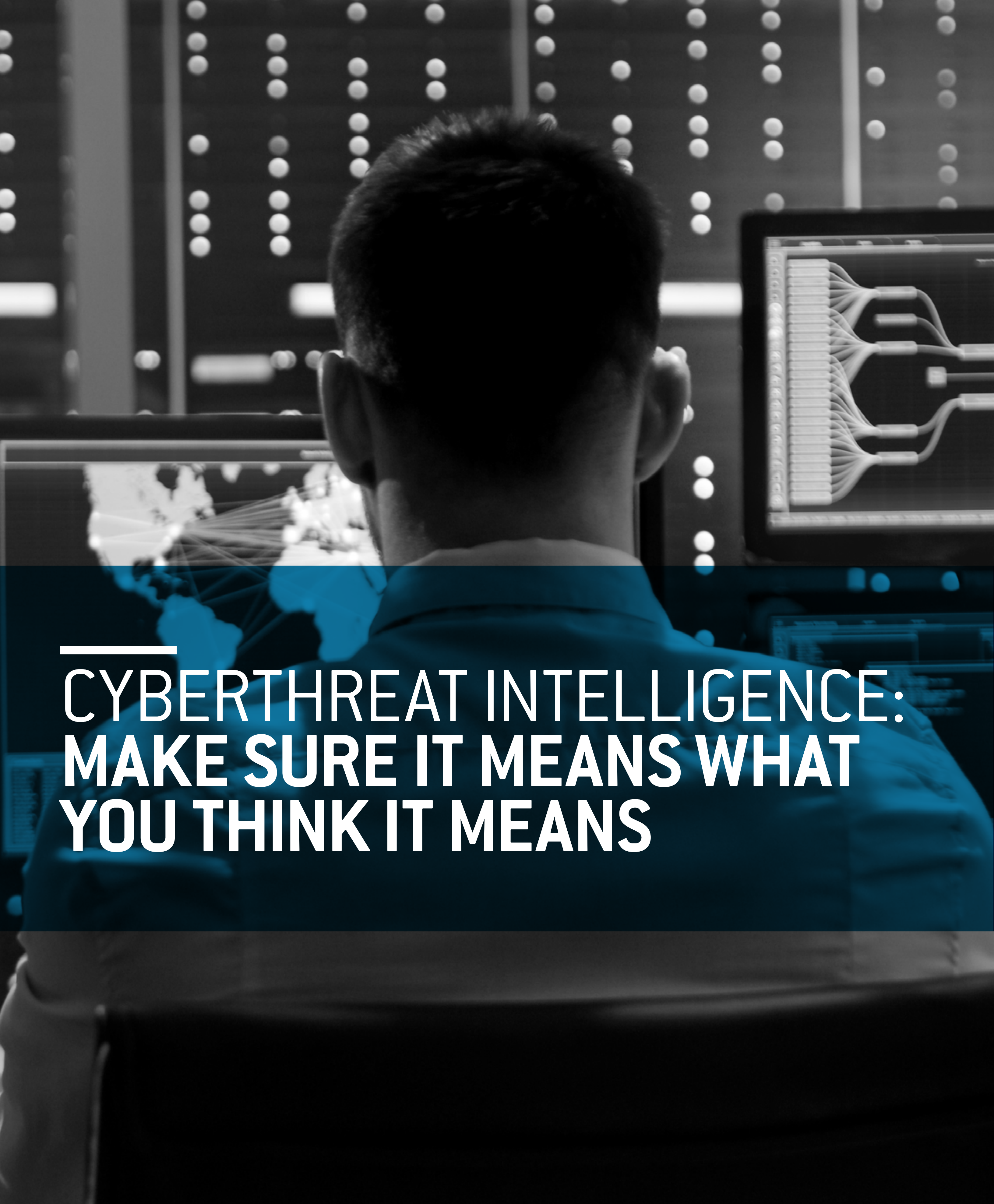
Like the settlers who moved to the western frontier, these countries apply custom tools and ramshackle solutions. Legacy technical hardware, applications that are very hard to support, and even unusual operating systems are commonplace. Robust network infrastructure, capable staff, and common equipment such as USB devices, are less common.

This makes it difficult but not impossible to provide technical solutions to these countries. However, when you can provide solutions, the ones used with mature markets won't normally work. Most of the time the customers in this type of market are governments, banking institutions, and other foreign partners doing business alongside you.

Lee Sult

Chief Technology Officer, Horangi

Lee is a seasoned incident response and cybersecurity consultant working on criminal matters as well as securing large enterprises. He spent time at Nuix, Palantir, and Trustwave.



CYBERTHREAT INTELLIGENCE: **MAKE SURE IT MEANS WHAT YOU THINK IT MEANS**

Imagine two pilots floating above the treetops in a hot air balloon. Out of nowhere, a gust of wind whips them far from their intended course. After hours of trying to divine their location, they drift low enough to grab the attention of a bird watcher.

"Hey!" one of the pilots exclaims. "You there! Can you tell us where we are?"

The birder responds, "You're in a hot air balloon."

The pilot sinks down in the basket, forehead in his palm. "Just our luck," he says. "The one guy we find had to be an intelligence analyst."

The other pilot asks, "What makes you think he's an intelligence analyst?"

"Because his answer was prompt, accurate, and of no use whatsoever."

As a former military intelligence officer, I know plenty of other jokes about intelligence and the people who provide it. In the military lexicon, there are generally two types of mission results: "operational successes" and "intelligence failures."

Outside the military, the concept of intelligence ricochets about the corporate world as if it's the greatest thing since two-ply toilet paper. In the world of cybersecurity, "threat intelligence" has become more than a buzzword; it's a fully functioning—and quite profitable—business line.

> *"Many people still think cybersecurity is an issue best kept to the folks in IT and reported on as needed to demonstrate "compliance." However, this mindset will not protect you from malevolent outsiders. More than likely, it won't satisfy regulators and plaintiffs' lawyers, who are becoming increasingly savvy at defining corporate cybersecurity obligations."*

This should come as no surprise; cybersecurity is full of military terminology. For instance, an organization that suffered a breach isn't the victim of "cyberassault" but rather a cyberattack. It's the victim of a forcible strike from an unseen adversary using complicated weaponry that damages its operations, systems, or finances. And if that's the case, the organization should prepare itself as the military does, by gathering and applying intelligence.

The trouble is, the business world has adopted the word "intelligence" without understanding what it really means. Gartner describes cyberthreat intelligence as:

"... evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

That's a lot to digest and many organizations gloss over some important elements or even fundamentally misunderstand what, exactly, cyberthreat intelligence is. As an attorney, I think this could be downright damaging.

Many people still think cybersecurity is an issue best kept to the folks in IT and reported on as needed to demonstrate "compliance." However, this mindset will not protect you from malevolent outsiders. More than likely, it won't satisfy regulators and plaintiffs' lawyers, who are becoming increasingly savvy at defining corporate cybersecurity obligations. Each organization must address the specific cybersecurity threat landscape that it faces. Quite frequently, cyberthreat intelligence is a key component in meeting that obligation, as long as the organization makes appropriate efforts and with appropriate resources. Let me explain.

RELATIONSHIP OF DATA, INFORMATION, AND INTELLIGENCE

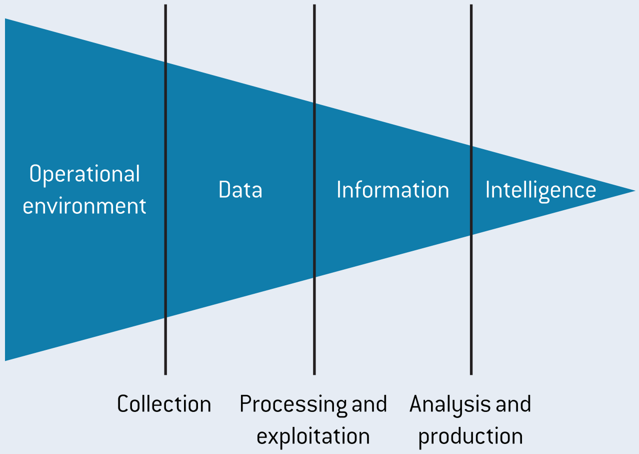


Figure 1: Relationship of data, information, and intelligence. Source: U.S. Department of Defense Joint Publication 2-0: Joint Intelligence

Each organization must address the specific cybersecurity threat landscape that it faces. Quite frequently, cyberthreat intelligence is a key component in meeting that obligation, as long as the organization makes appropriate efforts and with appropriate resources.

WHAT IS INTELLIGENCE?

In the military, "intelligence" is raw data processed into intelligible information and applied to a commander's mission alongside current information and past experience. The Department of Defense's Joint Publication 2-0: Joint Intelligence describes intelligence as the product of the process in Figure 1.

Notably, analysts need to compare information against other information before arriving at a specific conclusion. Moreover, the purpose of this exercise is not to inform the recipient of intelligence about what happened or why—that's called journalism. Rather, intelligence is a product that allows a decision maker to anticipate future circumstances and facilitates informed decisions by "illuminating the differences in available courses of action."

It's also important to recognize what intelligence isn't. As a product of analyses, it is not an exact science. In fact, the Joint Publication notes that:

"... intelligence analysts will have some uncertainty as they assess the Operational Environment, as should the commander and staff as they plan and execute operations. Intelligence, as the synthesis of quantitative analysis and qualitative judgment is subject to competing interpretation."

The bottom line is that intelligence is not an answer—far from it. Intelligence is simply a tool that allows leaders to make informed and hopefully successful decisions.

SOURCES AND METHODS

Most organizations subscribe to a stream or two of cyberthreat intelligence. That's an incredibly important first step. It's impossible to know what's coming at you if you're blind to the threat. Cyberthreat intelligence services provide a flow of intelligence about known, existing, and developing threats. The challenge is finding the right mix of intelligence sources for your needs.

Here again the military provides insight. Military intelligence is a product of multiple sources: imagery, signals, humans, and technical applications. Together they lead to predictive analysis that commanders use to make decisions. Along the way, analysts can choose the sources they need (or that they have access to) and can seek additional sources to obtain a more complete picture. If they think something is happening at a particular location, they can confirm or validate that belief from additional sources providing different angles or context. Each source of intelligence has its particular strengths, weakness, and veracity. Analysts must synthesize these sources to come to their conclusions—a product of seeing, hearing, telling, and feeling what is happening.

You may want to take a similar tack and examine threat intelligence from multiple sources in a way that allows each to complement the other and provide a robust picture of potential threats. To do this, you will first need to understand your organization's specific concerns, risks, threats, and data needs. That way you can choose and tailor threat intelligence solutions to address particular business problems.

It's important to recognize that threat intelligence feeds are not, as the name suggests, "intelligence." They're data. To transform them into intelligence, you must first process them through the lens of your organization to provide the necessary context to make it useful in decision making. Many organizations recognize this fact but still fail to analyze the data effectively. That takes something threat intelligence feeds can't provide: people who understand the data and your business.

THE HUMAN FACTOR

Choosing the right mix of threat intelligence feeds is not enough for a successful threat intelligence program. In fact, just subscribing to feeds may be more harmful than helpful. Your organization may not be able to make security decisions due to the fog of data without context.

As the Joint Publication notes, intelligence is not just about sources, it's about the people who review those sources. Intelligence analysis is not, and should not be, a one-person job. If you just thrust streams of threat intelligence at Jeff in IT, Jeff will explode. You need the benefit of different perspectives.

In addition, having a team of internal or dedicated professionals better positions the organization to address its specific business needs. Threat intelligence vendors can only customize their product so much to a particular client or industry. It's up to you to take that product to the next level, to operationalize that intelligence.

This requires individuals who understand how to use the incoming information to prevent, detect, respond to, and recover from a cybersecurity incident. Each of these functions is unique and no one set of skills will apply across the board. To be useful, intelligence must provide predictive and analytical insight leaders need, when they need it. For example, providing potential courses of action for a breach will not likely help leaders answer questions about prevention and detection.

A LEADERSHIP TOOL

Finally, most people lose sight of the fact that intelligence is a tool to help leaders make decisions. Therefore, it must get into the hands of leadership. More often than not, threat feed information (subscribed to at no cheap cost) is cultivated into intelligence by the organization's experienced staff (employed at no cheap cost) but never leaves the IT department. Not to speak ill of IT, but, honestly... Can the IT department make organization-wide decisions to address cybersecurity posture? Can the CIO act unilaterally to account for a new threat? Will the CEO and VP of Sales understand why entire segments of the organization have shut down to address potential threats?

Unless the answer to all of these questions in your organization is a resounding "yes," the customer for threat intelligence must be the C-suite. Furthermore, there may be many different customers depending on the product and its intent. An organization that properly uses cyberthreat intelligence will be able to identify which feeds will create which products to deliver to which internal customer. The alternative, treating cyberthreat intelligence as a one-size fits all solution, will then lead to an expensive cacophony of alarms and false positives that are more likely to drive a person mad than inform any decision.

Accordingly, you need to communicate any cyberthreat intelligence product to the people who can apply it. This means the organization must map who needs to know what. Each recipient must understand why they are receiving it and what they're permitted to do with it.

When dealing with cyberthreats, there are many unknowns. There are even, as former United States Secretary of Defense Donald Rumsfeld famously said, "unknown unknowns." Cyberthreat intelligence feeds are the tool of choice for many people who face these unknowns. But it is important to remember that subscribing to a feed is not enough. You also need people who can use it and leaders who are prepared to act on it. If you don't, you're just paying a lot for noise and woefully false sense of security.

Alexander Major

Partner, McCarter & English, LLP

Alexander focuses his practice on federal procurement, cybersecurity liability and risk management, and litigation. He is a prolific author and thought leader in the area of cybersecurity and a retired U.S. Air Force intelligence officer.

06

SECURITY DEFENSES

Our respondents are clearly masters of their craft, if you ask them. Even so, they're not infallible. We asked how often they found systems they couldn't break into and how effective their targets' defensive countermeasures were (figure 1).

More than half of respondents (59%) said they only encountered systems they couldn't break into less than 15% of the time. Only 9% of respondents said they found target systems they couldn't break into more than half the time.

We also wanted to know if there were ever times they were impressed by an organization's security posture (figure 2). The short answer: Only rarely did they find what they would consider effective security countermeasures.

WHICH SECURITY COUNTERMEASURES AND PROGRAMS ARE MOST EFFECTIVE?

If you're wondering what you can do to defend your organization better, our respondents weighed in on which security countermeasures they believed were the most effective (figure 3). Their opinions carry a lot of weight, given many of them spend all day every day trying to circumvent these security systems.

Just over one-third of respondents (34%) said host system hardening yielded the best results (which is great, cuz it's free, but time consuming). This was followed by intrusion detection and prevention systems at 18% and endpoint security at 14%. Honeypots or other deception technologies netted 10%, while Microsoft's Enhanced Mitigation Experience Toolkit (EMET) came in at only 8%, tied with antivirus. The lowest percentages were firewalls at 5% and Microsoft's User Account Control security framework at 3%.

These fascinating numbers provide a stark contrast between the security countermeasures organizations believe are impactful and what attackers themselves know to be true. Firewalls and antivirus solutions are required by most regulatory and compliance regimes, yet according to our data, they are all but useless (except maybe at keeping out the script kiddies). Of course, these technologies can be effective when combined with others (sort of like the commercials we saw as kids for sugary breakfast cereals being part of this complete breakfast), but apparently organizations are not using them properly.

It's great to see so many respondents voting for host system hardening, which includes security basics such as patches and updates and, again, costs nothing but your time. This is something we've seen through media coverage of recent attacks and ransomware outbreaks (not to mention my personal experience with close to 2,500 breach investigations)—the most effective attacks are those that take advantage of missing patches and outdated systems.

So, it looks like organizations are not using the countermeasures that have the greatest impact but focusing on those that have the least impact. That is really interesting and really frustrating. How can we as a professional body reclaim the ground we have surrendered to the adversary when we still struggle to get the basics right?

Last year, we also identified a disconnect between the security programs that executives believed were effective and those that hackers saw having an actual impact on their ability to break into systems. This year was no different (figure 4).

Not surprisingly, for the second year in a row, the vast majority of our respondents said goal-oriented penetration testing was very impactful (53%) or absolutely critical (26%) to an organization's security posture.

When I was presenting the results of last year's Black Report, people asked me if this was sample bias—ask a pentester if pentesting is important and of course they'll say it is. However, in my opinion this an accurate representation of fact. It's no different than asking a doctor if smoking is harmful to your lungs or asking an athlete if regular exercise improves your performance. In this case, how can an organization expect to mount any sort of meaningful defense against an attacker without engaging in regular attack simulations? Hint: They can't.

A whopping 73% of respondents said bug bounty programs were somewhat or very impactful but only a small proportion (12%) rated them as critical. More than half (58%) said employee education was very impactful or absolutely critical. Only 18% thought employee training was not really helpful in defending an organization. Since the attack surface extends to every employee in an organization, this is not surprising.

Somewhat more controversial was vulnerability scanning. One in five respondents (22%) said vulnerability scanning was an absolutely critical part of an organization's security posture, while 27% rated it very impactful and 36% called it somewhat impactful.

When I have met with customers to discuss this very topic, I have witnessed a disturbing trend; many people use the terms penetration testing and vulnerability scanning interchangeably. To be clear, a goal-oriented penetration test and a vulnerability scan are most certainly not the same thing; they have different purposes with different goals carried out by different people using a different set of tools. A vulnerability scan uses automated tools to make predefined checks for the presence of known security flaws and misconfigurations . Goal-oriented penetration tests are carried out by human beings that emulate the actual attack vectors that would be used by a criminal hacker.

One area where we saw a significant shift from last year was in respondent's opinion of information governance or data hygiene. Last year, 42% of respondents said these measures were not important but this year only 22% didn't see the need for it. By contrast, this year 30% believed it to be very impactful and 19% said it was critical.

This makes complete sense to me: How can you defend something when you're not entirely certain where "it" is? Another hint ... you can't. While some security professionals begrudge their information governance counterparts, I believe they are a critical member of the security team and provide valuable insight and perspective into the organization of sensitive data.

ORGANIZATIONAL SECURITY POSTURE

As a former chief information security officer and consultant with 15 years of experience, something that has always baffled me is the theory that security tools should be diversified. The argument goes that you should purchase a wide range of tools to have "best in breed" solutions. This makes sense on the surface: If one vendor's technology misses a particular malware or attack type, hopefully another vendor's will catch it.

However, all these tools have different user interfaces; alert in different ways; require different expertise to install, maintain, and monitor; and very likely don't communicate with each other very well (if at all). When cobbled together, they turn into a Security Frankenstein—an unmanageable monster that comes back to bite its creator.

They also require a security information and event management system or a human being to monitor each of them and correlate every alert on every system in an effective way that tells a story of what is actually taking place. This requires a level of technical acumen and intellectual capability that I simply have not seen in my 20 years in the industry. When you look at it from an operational level, diversification doesn't make much sense. As security professionals, our ultimate goal should be to minimize the number of tools we rely on and, if possible, interact with them all through a single pane of glass.

Our respondents shared these concerns (figure 5). More than one-third said integrating and orchestrating multiple security solutions from multiple vendors presented a high or medium-to-high risk to the organization. Only 6% said this was a low-risk approach.

1. HOW OFTEN DO YOU ENCOUNTER ENVIRONMENTS YOU CAN'T BREAK INTO?

Always	2%
More often than not (50–90%)	7%
Less than half the time (15–50%)	29%
Rarely (5–15%)	59%
Never	3%

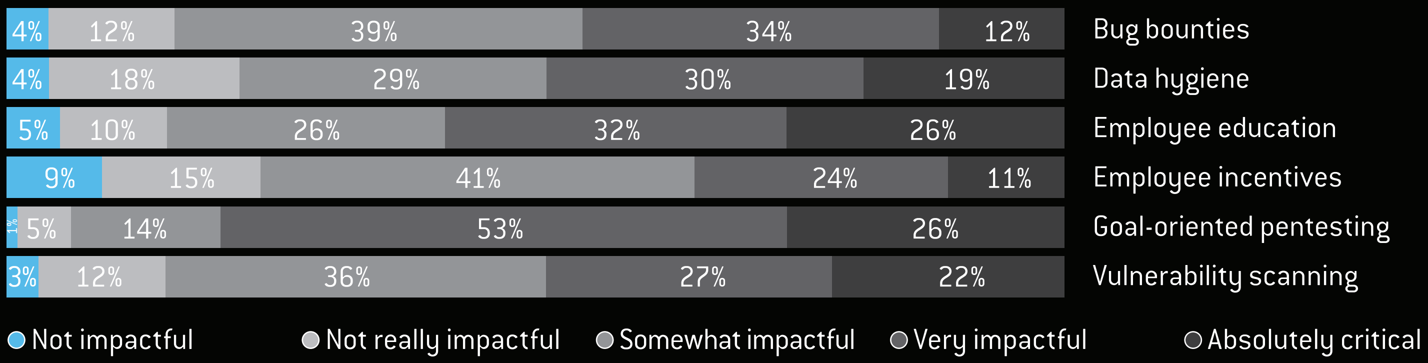
2. HOW OFTEN ARE YOU IMPRESSED BY AN ORGANIZATION'S SECURITY POSTURE?

More often than not (50–90%)	5%
Less than half the time (15–50%)	16%
Rarely (5–15%)	74%
Never	5%

3. WHICH SECURITY COUNTERMEASURE PRESENTS THE GREATEST CHALLENGE TO YOU DURING A PENETRATION TEST?

User Account Control	3%
Firewalls	5%
Antivirus	8%
Enhanced Mitigation Experience Toolkit	8%
Honeypots/deception technologies	10%
Endpoint security	14%
Intrusion detection/prevention systems	18%
Host system hardening	34%

4. RATE THE IMPACT OF THESE SECURITY PROGRAMS IN PREVENTING CYBERATTACKS



5. WHAT'S THE LEVEL OF RISK IN INTEGRATING OR ORCHESTRATING MULTIPLE SECURITY SOLUTIONS?

High risk	6%
Medium-to-high risk	33%
Medium risk	43%
Medium-to-low risk	12%
Low risk	6%

THERE AND BACK AGAIN: A FORENSICATOR'S TALE

Just as Bilbo and Frodo Baggins travelled across Middle Earth and back to the Shire, so have Nuix investigators gone there and back again. Over the past 12 months, Nuix investigators have seen the same themes and practices, again and again, leading to a breach. What is old is old … but still effective.

It's funny how organizations, after they're breached, almost always announce that it was a complex and advanced cyberattack the likes of which nobody has ever seen before. As a consultant, responding to breaches in organizations of all shapes and sizes, I have hardly ever witnessed extravagant, zero-day, or exceptionally complex attacks. They're out there, sure, but what we routinely see is a lack of data hygiene, misconfigurations, or problems with situational awareness.

The following nine common security issues continually reappear. I call them the wraiths of information security in honor of the nine who pursued Frodo for the One Ring. Everyone knows them by legend or lore but hardly anyone believes they are real in their worlds. Are they lurking in your environment, calling to their Dark Lord?

THE FIRST RIDER: SINGLE-FACTOR AUTHENTICATION

Over the past year, we've seen multiple clients with externally exposed or cloud systems that did not have two-factor authentication enabled. It was possible that the client had not enabled it for one reason or another and also didn't log or monitor attempts to access these resources. This is the ideal setup for brute-force attacks that, in some cases, were so successful they led to a full network breach. Attackers have huge lists of username and password combinations. All they need is for one to work.

To defeat this wraith, all internal and external systems that contain critical business information, personally identifiable information, health information, or financial records should have two-factor authentication enabled and logging on all access attempts.

THE SECOND RIDER: UNPATCHED SERVERS AND APPLICATIONS

We routinely encounter organizations running servers or applications with known vulnerabilities and with working exploits against those vulnerabilities. Common examples include WordPress and ColdFusion websites, servers running a version of the bash shell that can be ShellShocked, and organizations not testing or tracking their internal system or application inventories. Or, if they were tracking, the time from system regression testing to installation wasn't fast enough to keep out a wily attacker.

Defeating this wraith requires constant diligence with keeping abreast of security challenges as they arise and performing a risk assessment against your own assets.

THE THIRD RIDER: WEAK OR DEFAULT PASSWORDS

Amazingly, we still run across applications using default passwords or easily guessed variations. Any worthy adversary will try admin/admin to log into your application server and micros/micros on a fresh install of the Micros point-of-sale platform. Why waste time on more complex hacks if all they need to do is enter a default or weak password. Changing them to micros/M1cr0$ will not make their challenge any more difficult. Remember those lists of default passwords? They're trivially easy to try out against your infrastructure.

What will this wraith find in your shadows? You could do worse than implementing the National Institute of Standards and Technology's recently updated Special Publication 800-63. NIST recommends using passphrases comprising multiple unrelated words. Passphrases are easier for users to remember than the password policies of old (uppercase, lowercase, numbers and special characters) and, it turns out, are much harder to crack.

THE FOURTH RIDER: ANTIQUATED OPERATING SYSTEMS

Antiquated or end-of-life operating systems that can no longer obtain security or software patches need to disappear or have compensating controls. Risk managers should understand that a $1 million tool such as a microscope (true story) may be essential to our business but if it only runs on Windows XP, it will need a fellowship of the ring, such as network segmentation or jump hosts, to protect that which cannot protect itself.

THE FIFTH RIDER: OVERPRIVILEGED USERS

Despite your best efforts, it turns out you can't operate a business without users or replace them all with machines. But they don't all need to be local admins or, worse, domain admins. Giving users privileges they don't need only makes the attacker's job easier—they don't even have to bother using privilege escalation techniques.

To defeat this wraith, best practice is to separate standard user accounts from privileged accounts. In fact, several frameworks and standards require it. Think of it as another layer of your security model. Apply the principle of least privilege, in other words, only give users the privilege they need to do their jobs.

THE SIXTH RIDER: NON-WORK-RELATED ACTIVITIES

Are you tracking what users are doing with corporate assets? Are they playing Candy Crush? Checking the progress of their fantasy football teams? Downloading pirated software or movies? How do you know?

Everywhere a Nuix Investigator has gone in the past 12 months, we've found examples of non-work-related activities on critical or breached systems. This is especially hazardous when combined with users who have excessive privileges.

Take back your network by deploying controls over what users can and can't do. Almost all organizations have acceptable use policies but historically they've lacked enforcement, technical controls, or instrumentation to monitor. Cast these users back into the wraith world.

> *"It's funny how organizations, after they're breached, almost always announce that it was a complex and advanced cyberattack the likes of which nobody has ever seen before. As a consultant, responding to breaches in organizations of all shapes and sizes, I have hardly ever witnessed extravagant, zero-day, or exceptionally complex attacks. They're out there, sure, but what we routinely see is a lack of data hygiene, misconfigurations, or problems with situational awareness."*

THE SEVENTH RIDER: ROLLING YOUR OWN SOFTWARE

If you are not a software company, with teams of developers, quality assurance personnel, or application security personnel, you should probably not try to re-invent the wheel by rolling your own software. We've seen organizations building their own encryption tools even though tested and vetted algorithms are already available. We have seen stores make their own payment applications even when their payment processors or systems integrators already had certified platforms. This wraith loves to lurk inside your home-grown applications.

Sometimes it makes sense to roll your own software to meet a specific organizational need. If you do, make sure you test it, vet it, and review it before deploying into production. If you don't, you'll likely get plenty of "free" testing from the less savory corners of the interwebz.

THE EIGHT RIDER: NO NETWORK SEGMENTATION

In our journey there and back again, we've seen environments where employees were playing Candy Crush on computers in the same network segment as every point of sale terminal.

Segmenting off networks that contain the corporate "crown jewels," intellectual property, personally identifiable information, or other sensitive data from general-purpose networks forces an adversary to shift tactics, techniques, and procedures. Several compliance frameworks require you to use segmentation as a security boundary for identification and protection of sensitive data.

Segmenting your networks also allows you to instrument appropriately to gain insights into who is poking around your most prized or controlled data. It also provides natural choke points to restrict data flows into and out of that environment.

THE NINTH RIDER: LACK OF INSTRUMENTATION

Last, but certainly not least, do you have the instrumentation in place now for when an incident occurs? In almost all the breaches we investigated, the victims lacked visibility into crucial aspects. One had logs, but only three weeks' worth. Another had no logs or instrumentation at all. My favorite had implemented an endpoint detection and response solution but it was still in learning mode when the organization got breached. The EDR systems actually learned that being pwned was normal activity!

To see this wraith coming, organizations need visibility into their networks, traffic, endpoints, and sensitive data to make informed decisions about the state and well-being of their environments. When you get breached—it's when, not if—robust visibility will reduce your time to identification and time to response.

ONE RING TO RULE THEM ALL?

It's not enough for us to identify recurring themes across responses. Collectively, organizations need to take ownership of their environments, take initiative to identify their gaps, and take stewardship of the data they hold dear. Security is only as strong as the weakest link in the proverbial chain. If the past 12 months are any indicator, we are walking the same roads over and over again, making the same mistakes.

Jim Rouse

Chief Information Security Officer, Gemini

Jim is a former Special Agent of the Naval Criminal Investigative Service and a former member of Nuix's Cyber Threat Analysis Team. He has extensive experience in forensics, incident response, eDiscovery, litigation support, breach investigations, insider threat investigations, security auditing, security architecture, and payment card forensic investigations.

MACRO VIRUSES: **WHY ARE THEY STILL A THING?**

Just over 20 years ago today I got my first job writing about technology—it ended up being a career. Working in and observing the IT industry for so long has given me insights into how fast some things change and how others stubbornly stay the same. Over the past 20 years, macro viruses have been a constantly evolving but constantly present menace. The reasons for this also explain why cybersecurity in general is so hard to get right.

WHAT EVEN ARE MACRO VIRUSES?

Not long after I started as a journalist, the Melissa virus hit the headlines. It wasn't the first macro virus but it was the first really good one.

The payload was a Microsoft Word document with … boy does this sound familiar … a malicious macro that connected to Microsoft Outlook, extracted the first 50 names from the user's address book, and emailed itself as an attachment to those 50 people. Even though its social engineering techniques were laughably primitive by today's standards, some of those people went "Oh, Josh emailed me this document and said it was a secret; I'd better open it!"

Melissa very quickly went viral, spreading all over the world in a few days. (A year later, the ILOVEYOU worm managed the same feat in a matter of hours.) But that's all Melissa did. It didn't encrypt your files, backdoor your PC, or steal your data. It just replicated itself by email.

Most individual victims didn't suffer much, except those whose internet providers charged by the email message (that was a thing back then). But you can imagine the network effects that happened once Melissa got inside corporate networks. Plenty of enterprise and government email servers were completely overloaded and had to be shut down and rebooted or rebuilt. (You kept backups, right?)

IT'S NOT MY FAULT

Tech industry commentators (me included) said unkind things about dumb people who opened attachments that were obviously some kind of malware. We also, quite rightly, pounded Microsoft for building all this functionality into its products without considering how someone could abuse it from a security perspective. Like, a Word document that could access your Outlook address book and send emails, as if that could never go wrong? Duh. In hindsight.

Over the next few years, Microsoft took serious steps to address security issues in its operating system and office applications. It hired a bunch of cybersecurity guys who wore earrings and unconventional haircuts and t-shirts rather than suits. (Hoodies hadn't been invented yet.) It changed its development practices and invented Patch Tuesday. It made all those annoying pop-up messages pop up every time you tried to do anything.

And yet … and yet … almost 20 years after Melissa, macro viruses are still a thing. And we're still arguing about whether people or technology are to blame.

MACRO VIRUSES—AND DEFENSES—HAVE EVOLVED

Nowadays it's a little more complex. Multiple layers of antivirus technology at your email provider, server, and desktop should catch any email attachment containing a macro virus. However, malware authors use a variety of tricksy techniques such as polymorphic obfuscation to fool the antivirus. (It also makes it hard work trying to figure out what these macros do. According to Nuix malware analyst Andrew Spangler, this is "almost as much fun as punching yourself in the eyeball with your elbow.")

As a result, you sometimes still get an email with an attachment from someone you know. Or someone pretending to be someone you know (it can be hard to tell). You remember something from a training course about not opening email attachments but this one is from your CEO! Or it says your internet will get shut off if you don't pay the bill pronto! So you open the attachment and … nothing happens.

Microsoft Word has recognized that this document is an email attachment that may contain malicious software and blocked it from running macros. However, the content of the document is blurred and there's a message saying that to view it you need to click the "enable content" button at the top of your screen. You click the button and bam, you've just downloaded and executed ransomware. Or a Metasploit module. Or whatever other malware someone wants to run on your system to pwn your data, or your organization's data.

"Word documents were built not just to contain text and static content but also to leverage other features of the operating system," explained Josh Mitchell, a security researcher at Nuix. "You can embed an Excel spreadsheet, a video, a Flash animation—the surface area is huge. The only thing we have from an end user standpoint is a warning."

CAN'T WE JUST GET RID OF MACROS?

OK, that being the case, why not just prevent Office documents from running macros at all? Who even needs them?

Problem solved. Well, not quite.

"Most corporate environments where these things are being targeted, people still think about networks as a hard outside and a soft, squishy inside," said Mitchell. "So they have external-facing stuff secured but the patch management on the client side usually lags behind.

"That means even if you disable macros, there are still code execution bugs that malware can leverage—although those are harder because you need to have a better understanding of the environment the exploit will be running under. There are also DDE bugs, using Dynamic Data Exchange rather than Visual Basic to execute commands."

BUT I NEED MY CUSTOM APPLICATION!

In addition, many companies would grind to a halt if they couldn't run macros. In most large organizations, employees or teams build custom workflows into their office document templates to automate common processes.

"A lot of the time, these macros are developed as shadow IT projects by someone who's done a bit of Visual Basic for Applications," said independent security researcher Troy Hunt. "It's all available there in Excel or Word, it's familiar, and it's easy to stand up. People start using it, it gets traction, and eventually it's something everyone depends on, even though it's built on a foundation we know is terribly insecure."

Once a custom application becomes popular, it can be difficult to kill off.

"Your IT department could just block VBA or macros at a Group Policy level but then what happens to the employees who need that application?" said Hunt. "They'd have to pay a vendor to build it again more securely. Then the developer decides that since it's behind the firewall, it's safe, so they end up making the same bad design decisions again."

ATTACHMENTS ARE SO LAST WEEK

Alright, instead of blocking macros, how about removing attachments entirely?

"I worked at one place where they scrubbed all external attachments and it was a really effective way of mitigating most of these types of attacks," said Mitchell. "But you have to take into consideration that some departments such as marketing and human resources can't work without attachments, so you need to work around that by segregating those networks."

CYBERSECURITY IS TOTES HARD

This is just one example of how IT departments must balance security with productivity, cost, and many other factors.

"IT guys have a big backlog of things to do, performance enhancements, new releases, and they need to need to prioritize them," said Hunt. "With security issues, they need to balance the likelihood of a successful attack and the impact that would have.

"In a perfect world, they'd be aware of the potential risks and make a rational decision to fix it or not to fix it. However, sometimes it just gets put in the too-hard basket."

SO, LIKE, WHAT CAN I DO?

Two decades after Melissa, macro viruses are still a thing. And they'll probably still be a thing 20 years from now. However, you can minimize the damage they can cause. The Australian Signals Directorate's guide to Microsoft Office macro security recommends one of three approaches:

- Disable all macros
- Allow only macros from controlled trusted locations
- Allow only digitally signed macros.

Each approach has pros and cons for security, business impact, and difficulty of implementation. You need to decide which one is right for your organization based on these factors. ASD also recommends implementing:

- Application whitelisting to prevent a malicious macro running unauthorized programs
- Email and web content filtering to inspect incoming Microsoft Office files for macros, and block or quarantine them as appropriate
- Macro execution logging to verify only authorized macros are used
- VBA training for users or IT admins assigned to assessing if macros are safe or not.

For a step beyond application whitelisting, advanced endpoint software such as Nuix Adaptive Security can block malicious behavior, for instance preventing a Word document from running any kind of executable. That way, you're protected against macro viruses, DDE bugs, and code execution bugs.

Josh Mehlman

Content Lead, Nuix

Josh has worked as an information technology journalist and communications specialist for 20 years. He collaborates with Nuix's subject matter experts to create marketing and thought leadership material including white papers, case studies, blog posts, brochures, videos, and fact sheets.

```
public function imgdeploy()
{
    $PR = Product::select('id', 'image', 'mirror')->where

    $bar = new ProgressBar($this->output, $PR->count());
    $bar->setFormat('debu                          ()->setBarW

    $prod
    $
            . $product->imag

     _contents(config('app.u
    ublic_path('imgs/produc

    params->unique('name')
    nts->where('id', $par->
    t' => $var->sort, 'name

    unique('name') as $par)
      ->where('id', $par->piv
        $var->sort, 'name'

        } else {
            $variant = $this->model->categories->first(
            $name = $variant->name_sngl;
            $gender = $variant->gender;
        }

        return (object)['name' => $name, 'gender' => $
    } catch (\Exception $e) {
```

STRATEGIES TO PROTECT AN INTERNET OF THINGS

Cybersecurity is rarely the first line item in a company budget. Often, executives only take it seriously after a major security event. Internet of things (IoT) devices are even further down the list of concerns. Even IT people typically dismiss them with “I wouldn’t worry about that device” or “You can’t do anything with that other than turn on a light.” This nonchalant approach makes IoT devices a perfect target for attackers.

IoT devices are simply everyday devices that have been given network access: a lightbulb you can turn on using your laptop; a thermostat you can adjust from your office so your house is warm by the time you get home; a car that is connected to the cloud and transmits diagnostic information to the dealer or manufacturer. All these devices started life with a singular purpose but as their functions and capabilities evolved, so did the vulnerabilities.

Every day, consumers and businesses plug IoT devices into their networks without a thought for security. Market analyst Gartner estimates 8.4 billion IoT devices will be used worldwide in 2018 and 20.4 billion by 2020. With this potential revenue stream in sight, device manufacturers are prioritizing speed—being first to market and establishing a foothold. If they think about security, it is usually at the end of the development process. Perhaps they hope to rely on “security by obscurity,” the idea that these devices will be hard to find and nobody will be interested in them.

Nonetheless, many people assume that any manufacturer putting a device on sale has tested it for safety. Common household and office products must comply with a raft of health, safety, and environmental protection standards such as Conformité Européenne in the European Union. Many manufacturers also submit products to certifying bodies such as UL (formerly Underwriters Laboratories) for testing. No such standards or certifying bodies exist for the security of devices. The responsibility, in most cases, falls to the end user who is not equipped or trained for the task.

This is why IoT is the wild west for hackers. Knowing these devices are vulnerable, hackers and security researchers learn how to identify them and trawl the web for unprotected IoTs. These devices will inevitably be looked at, probed, attacked, and exploited.

DANGERS OF IOT

One result of an IoT exploit was discussed in Verizon's 2017 Data Breach Digest. In 2016, a security admin at a university discovered that the IoT devices on its network—the college had internet-enabled thousands of devices including vending machines, lights, light sensors, and fridges—had become part of a botnet. Hackers had used brute force attacks to crack default and poor passwords. Once they had control of these systems, they deployed malware that told these devices to conduct DNS lookups for seafood restaurants. (Why seafood? Who knows?) This slowed down the network and prevented some web access but the IT staff remediated the issue before it took down the university's entire network.

The Mirai IoT botnet in October 2016 was on a much larger scale. Researchers from data security company Imperva analyzed the attack and tallied 49,657 unique IP addresses from 164 different countries. This attack involved internet-connected cameras, digital video recorders, and routers that used hard-coded or default usernames and passwords. Hackers used these to devices to unleash a distributed denial of service attack that collectively generated up to 1.2 terabytes per second of traffic. Targets included the website of security researcher Brian Krebs, French internet service provider OVH, Airbnb, GitHub, Netflix, Reddit, and Twitter. The code for the botnet was publicly released and hackers have since modified it to perform other attacks on IoT devices.

HOW CAN I SECURE MY DEVICES?

Good, basic network design principles will go a long way toward securing IoT devices. Some of the best things you can do are also the simplest, such as changing default usernames and passwords and disabling port forwarding. If a device uses a hardcoded username or password, there's not a lot you can do aside from reconsider if you actually need the device connected. Here are some other considerations.

1. Logging and auditing

Almost all network security appliances have logging capability built in but in many cases this is disabled or stifled. Make sure you correctly configure logging on your firewall and that someone regularly reviews these logs for anomalies. The university and Mirai IoT breaches I discussed were discovered, wholly or partially, by examining logs.

2. Educate users

Many people don't realize the consequences their actions can have on the network and ultimately to the financial stability of the company and the privacy of their data. Regular training sessions, email notifications, operational security posters, and live demonstrations help make people more aware of threats and more responsible for what is happening. It is the idea of taking ownership.

3. Segregate Your Network

The simple way to do this is to create a separate network for IoT devices, similar to a guest network for untrusted devices. It allows the device to access the internet but not to communicate with other devices that hold your critical data. Many network switches, routers, and wi-fi access points can do this natively. Alternatively, simply add another wireless router to the network and configure your main router not to allow traffic between the two networks.

For more complex environments, you can virtually segment devices on the same physical network using a virtual local area network (VLAN). Placing all your IoT devices on the same VLAN makes managing these devices less complicated. You can apply sufficient logging and use firewall rules to lock down IoTs so they have enough network access to complete their specific function but no more.

4. Document and Communicate

As you deploy IoT devices, it can be easy to lose track of what is connected to the network and where. IoT devices are often left out of IT update plans. Documenting your use of IoT and communicating this within IT staff can solve the problem. Documenting also reduces the likelihood that you'll miss IoT devices during an update or patch period.

DON'T BE AN EASY TARGET

Hackers will typically attack low-hanging fruit—devices or systems that require the least effort to achieve their goals. IoT devices are, for now, about the lowest hanging fruit you can find. Handling IoT devices using recognized and industry-standard security practices will help you secure these devices and the network as a whole.

For more detail on securing IoT, read:

- U.S. Department of Homeland Security, Strategic Principles for Securing the Internet of Things
- National Institute of Standards and Technology Special Publication 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
- National Institute of Standards and Technology Special Publication 800-183, Networks of 'Things'.

Peter Evans

Senior Information Security Consultant, Nuix

Peter has more than 10 years' experience in federal law enforcement and another 10 years' experience as an information technologies and radio frequency engineer. While working in law enforcement, Peter was detailed to the Electronic Crimes Task Force and was the lead forensic investigator on computer crime, network intrusion, and wireless exploitation cases.

WHAT HAPPENS AFTER AND WHAT DO YOU TELL THE BOARD?

When I worked as a consultant, I would sometimes hear through back channels that the weaknesses or vulnerabilities my team had identified (which were directly tied to the cause of the breach) were not addressed. Of course, I was ignorant to the mitigating circumstances and myopically focused on my contributions but meh … I just didn't get it. I still don't. How can you leave a vulnerability in place that you know is part of the reason you were compromised? I mean, I get that there are competing priorities, but come on … this is 101 stuff. Is it really that hard?

Our survey showed this dynamic hasn't changed. The clear majority (93%) of respondents told us that after a penetration test, the client would most commonly not fix some or all of the vulnerabilities identified by the testers or investigators (figure 1). Only 7% would remediate all the vulnerabilities found and then re-test to see if they'd plugged all the gaps. I'd like to say shockingly, but I am a pragmatist, 18% said many of their clients would talk about what needed to be done but not actually do it, and 6% said their clients did nothing because the pentest was just a box-checking exercise or regulatory requirement.

Despite their frustrations, most respondents were optimistic and generous about their clients despite the steady stream of breaches in the news (figure 2). For almost half (44%), news of yet another breach makes them think it could motivate people to start taking security more seriously. For a similar number (43%), even if a company had lax security that doesn't mean it deserved to be hacked. A small proportion of hackers we surveyed, however, felt companies that suffered data breaches got what was coming to them due to their poor security measures or other activities of that company.

Clearly, there is a pervasive opinion that organizations could and should take security more seriously. While it does not mean they should be the victims of a crime, perhaps a renewed focus is in order.

FRAMEWORKS AND LEGISLATION

Many organizations operate within tightly defined industry frameworks such as ISO 27001, the Federal Information Security Act (FISMA), the Payment Card Industry Data Security Standard (PCI DSS), or the Health Insurance Portability and Accountability Act - Health Information Technology for Economic and Clinical Health Act (HIPAA HITECH). Ironically, perhaps, some industries that have heavy compliance burdens are among the easiest to break into and steal data from, according to the pentesters we surveyed (see Which Industries Have the Worst Security? on page 23).

Our survey showed that 57% of respondents felt these compliance frameworks were effective at reducing cybersecurity risks (figure 3). Considering how much money, time, and energy organizations in heavily regulated industries spend complying with these frameworks. I'm sure they would like to see the "yes" number be much higher.

In addition to industry frameworks, many state and federal governments are passing cybersecurity legislation. As well as the infamous European Union General Data Protection Regulation, there are breach disclosure laws in place or on their way in Australia, China, Japan, Mexico, South Korea, the United Kingdom, and the United States. The numbers here were almost identical to those about compliance regimes, albeit reversed (figure 4). Just over half of respondents (53%) did not think legislation would have a positive impact on security.

Respondents may have been influenced by the situation in the United States, where there are 48 different pieces of state cybersecurity legislation that don't seem to be all that effective. It's clear that governments have a role to play in preventing attacks and ensuring organizations report on them in a timely manner but the pentesters we surveyed were not very confident that it would work.

EXECUTIVES AND THE BOARD

Most hackers don't have many opportunities to sit down with members of their executive staff or boards of directors, so once again we gave them the opportunity to have their voices heard.

When we presented last year's Black Report to senior executives and board members around the world, many of these company directors told us they welcomed this sort of feedback. They believed it was essential for them to understand the security challenges they faced, the risk associated with those challenges, and the opinions of the experts of how to address them.

Since this was such a popular section last year, we didn't want to disappoint our readers!

Given the opportunity to sit down with a CEO (or any CEO), almost half (42%) of the hackers we surveyed would stress that security needs to become part of normal operations—it's a journey, not a destination (figure 5). Another third of respondents would like to explain that neither people nor technology alone can solve the cybersecurity problem, it needs to be a combination of both.

Just over one-third of respondents (36%) believed company directors understood the importance of security to the future of their business (figure 6). The remainder were more skeptical of the board's motives, indicating that board members were only addressing security for compliance reasons or to keep up appearances. A small number (3%) thought boards' heads were buried in the sand on security issues.

On the off chance that they could address the board, nearly half of respondents (43%) would warn them about the significant adverse impacts a badly handled data breach would have on the organization's brand and the need to be prepared (figure 7). The remaining respondents were fairly evenly divided around messages on the overall importance of security, the litigation risks involved in data breaches, and the idea that getting hacked is not an if or even a when—it's a current reality.

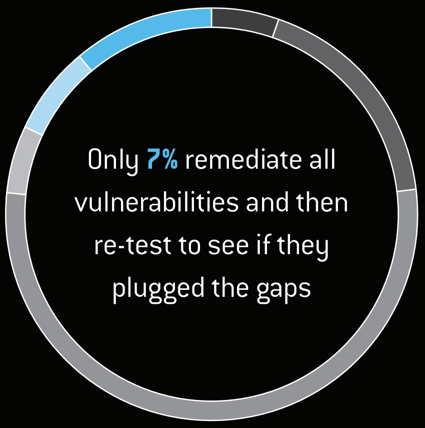
PROGNOSTICATION

Finally, we asked respondents to prognosticate a bit and give us their opinions on what were the most concerning future cyberthreats (figure 8). Their greatest concerns were SCADA attacks and ransomware, while the lowest were biomedical device, vehicle, and mobile device hacking.

This surprised me a little, given there were multiple stories last year about researchers being able to remotely access a vehicle's onboard computer systems and influence various aspects of its performance. As with many new internet-enabled real-world devices (broadly called the internet of things), automobile manufacturers have integrated technology into their products with more concern for being first to market than for security. Security professionals have taken much delight in finding the holes in these systems, but perhaps the potential for widespread damage is limited. Still, you wouldn't say that if you had to pay a ransom to start your car ... or your pacemaker.

Looking at it this way, SCADA and ransomware attacks are a big concern—a widespread attack by a terrorist organization or hostile nation state could be catastrophic. Sadly, I still firmly believe that we are careening towards a trigger event that will involve significant loss of human life.

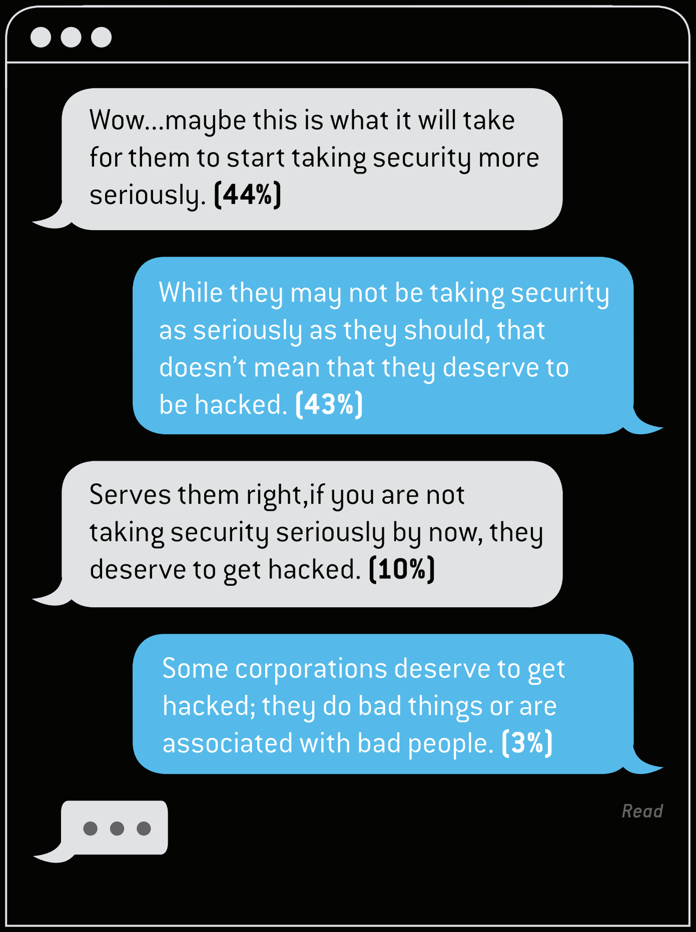
1. AFTER A PENTEST OR A BREACH, WHAT ACTION DO YOUR CLIENTS MOST COMMONLY TAKE?



Only 7% remediate all vulnerabilities and then re-test to see if they plugged the gaps

- ● A bit of everything
  11%
- ● Full remediation of all vulnerabilities and re-testing
  7%
- ● Extensive remediation of most identified vulnerabilities
  5%
- ● Some remediation; usually focused on critical and high vulnerabilities
  53%
- ● Talk about what should be done, but end up not taking any action
  18%
- ○ Nothing, they were merely checking boxes
  6%

2. WHEN I READ ABOUT THE LATEST SECURITY BREACH, MY RESPONSE IS USUALLY...



Wow...maybe this is what it will take for them to start taking security more seriously. **(44%)**

While they may not be taking security as seriously as they should, that doesn't mean that they deserve to be hacked. **(43%)**

Serves them right,if you are not taking security seriously by now, they deserve to get hacked. **(10%)**

Some corporations deserve to get hacked; they do bad things or are associated with bad people. **(3%)**

3.

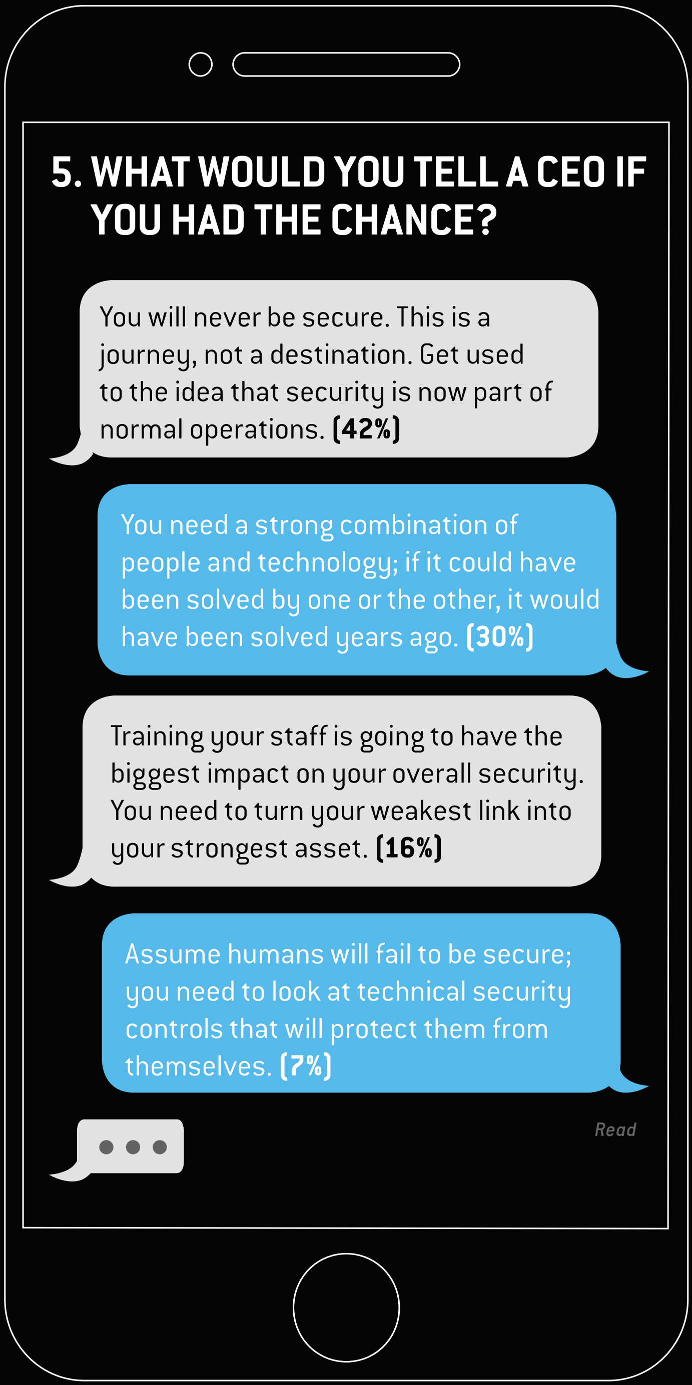
FIFTY SEVEN PERCENT

OF HACKERS THINK COMPLIANCE FRAMEWORKS SUCH AS PCI, THE NIST CYBERSECURITY FRAMEWORK, AND ISO 27001 ARE EFFECTIVE

4. DO YOU THINK CYBERSECURITY LEGISLATION WILL LEAD TO MEANINGFUL CHANGE?

👍 Yes
47%

👎 No
53%



5. WHAT WOULD YOU TELL A CEO IF YOU HAD THE CHANCE?

You will never be secure. This is a journey, not a destination. Get used to the idea that security is now part of normal operations. **(42%)**

You need a strong combination of people and technology; if it could have been solved by one or the other, it would have been solved years ago. **(30%)**

Training your staff is going to have the biggest impact on your overall security. You need to turn your weakest link into your strongest asset. **(16%)**

Assume humans will fail to be secure; you need to look at technical security controls that will protect them from themselves. **(7%)**

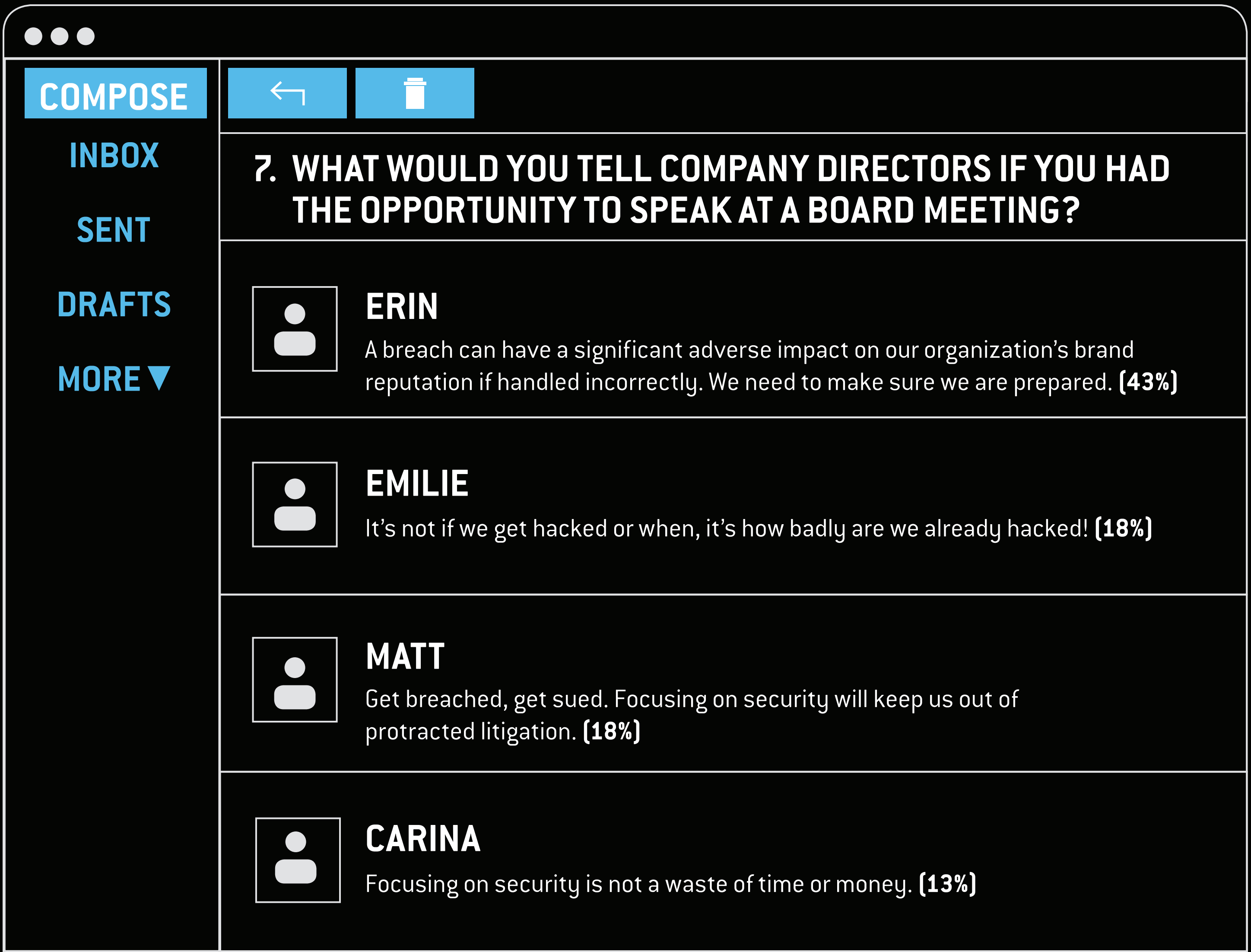
6. WHAT DO YOU THINK YOUR DIRECTORS WOULD SAY ABOUT THE IMPORTANCE OF SECURITY TO FUTURE BUSINESS?

We have to deal with security for compliance reasons, nothing more. **(33%)**

Security is important to us and to the future of our business. **(36%)**

Companies get hacked every day; it is the new normal. We should do just enough to show we think it's important, but no more. **(19%)**

Security is a waste of time and money. I don't need or want to know about it. **(3%)**



7. WHAT WOULD YOU TELL COMPANY DIRECTORS IF YOU HAD THE OPPORTUNITY TO SPEAK AT A BOARD MEETING?

ERIN

A breach can have a significant adverse impact on our organization's brand reputation if handled incorrectly. We need to make sure we are prepared. **(43%)**

EMILIE

It's not if we get hacked or when, it's how badly are we already hacked! **(18%)**

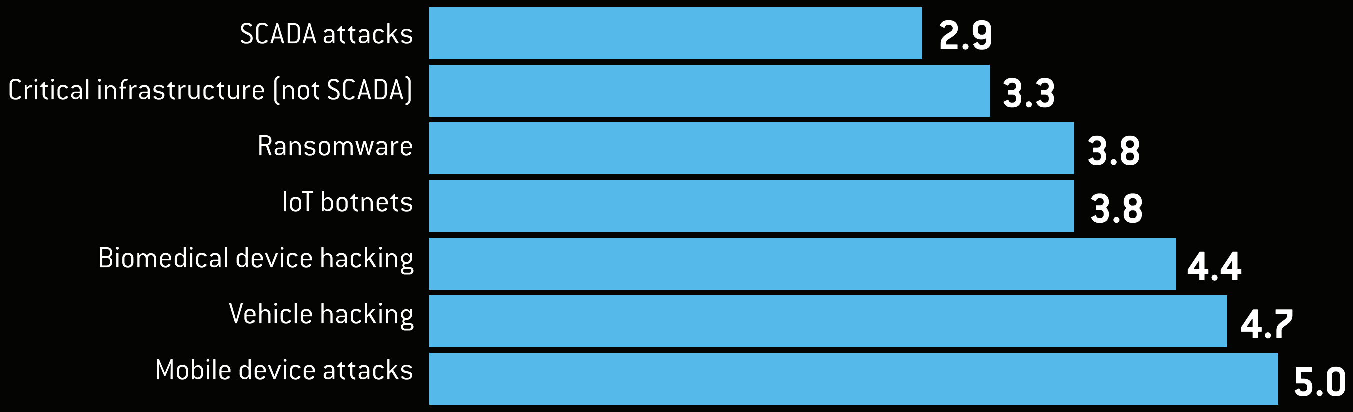
MATT

Get breached, get sued. Focusing on security will keep us out of protracted litigation. **(18%)**

CARINA

Focusing on security is not a waste of time or money. **(13%)**

8. WHAT DO YOU SEE AS THE MOST CONCERNING FUTURE THREATS?



Average Score for each option, lower score=more concerning

THE CONVERGENCE OF LAW AND CYBERSECURITY

The definition of "cybersecurity" hasn't changed much over the past 30 years. The term first emerged in the late 1980s to describe measures taken to protect a computer against unauthorized access or attack. The 2008 National Security Presidential Directive regarding Cybersecurity Policy (NSPD-54) defines it more specifically as: "[p]revention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

LACK OF UNIFORM POLICY

Despite (or perhaps because of) this relatively static definition, the legal risk in this area is higher than ever before. This is partly because cybersecurity law, policy, and practice are not fully developed. There is no uniformity between countries, states, or industries.

For example, once an organization suspects a data breach has occurred, it has a time window in which to identify what information was compromised, confirm that it has remedied the vulnerability, and notify the required individuals, law enforcement, regulatory agencies, and so on. This breach reporting deadline varies considerably depending on the type of data that was compromised and the applicable jurisdiction. For example, a contractor to the United States military has 72 hours to report the loss of covered defense information under Defense Federal Acquisition Regulation Supplement 252.204-7012. In contrast, an organization that loses personally identifiable information may have 30 days or 90 days after discovering a breach to notify US residents (depending on the state). The European Union's General Data Protection Regulation (GDPR) requires notice within 72 hours but Australia's Notifiable Data Breaches scheme allows 30 days.

THIRD PARTIES MAKE THINGS COMPLICATED

Responding to an incident is further complicated when the breach involves a third party. An external vendor may be less forthcoming with objective evidence that the breach was remedied, such as an independent forensic expert's report. Unsurprisingly, the concern is that an independent expert will draw conclusions on the cause and extent of the breach that may show the vendor was negligent.

In this scenario, an organization's legal team is not only concerned with who must be notified and when. In case of litigation with the vendor or consumers, it must also establish a record that shows it secured its network access to or from the vendor while awaiting confirmation that the vendor's breach was remedied. However, cutting off the vendor's access to your systems may pose legal issues as well—the vendor might file a temporary restraining order.

Even where companies make every effort to comply with data security and breach notification laws and regulations, there is no guarantee that an agency or court will find the company acted responsibly. And, these are just a few issues that might arise in responding to a data breach.

AN ENTERPRISE-WIDE (AND EXTERNAL) CYBERSECURITY TEAM

An organization's best defense is a good offense. This means adopting a whole-team, enterprise-wide approach to cybersecurity, rather than leaving it exclusively in the hands of your information security and information technology teams. It also requires outside counsel with cradle-to-grave cybersecurity expertise, including compliance audits, investigations, breach response and crisis management, privacy litigation, and responding to and defending against agency enforcement actions.

In the event of a suspected or actual data breach, outside counsel often plays the role of quarterback, responsible for calling the play. This is necessitated by the ever-changing legal landscape coupled with the risk tradeoffs between what an organization may be required to do versus what it should do.

This was evident in the post-breach litigation proceedings of organizations such as Yahoo! and Equifax. The courts of law and of public opinion have decided that it's no longer acceptable for an organization to fail to provide reasonable defensive

> *"Responding to an incident is further complicated when the breach involves a third party. An external vendor may be less forthcoming with objective evidence that the breach was remedied, such as an independent forensic expert's report. Unsurprisingly, the concern is that an independent expert will draw conclusions on the cause and extent of the breach that may show the vendor was negligent."*

countermeasures to protect customer or commercially sensitive data. The chasm between technical competence and legal or regulatory compliance has been bridged in such a way that breach fatigue has been replaced by frustration, incredulity, and sardonic cries for responsibility and action.

LEGISLATORS GET SERIOUS

In November 2017, Democratic Senators Bill Nelson of Florida, Richard Blumenthal of Connecticut, and Tammy Baldwin of Wisconsin proposed the Data Security and Breach Notification Act. The purpose of the bill is "To protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a breach of security." It also proposes a potentially game changing article in section 1041:

Concealment of breaches of security involving personal information 14 "(a) IN GENERAL.—Any person who, having knowledge of a breach of security and of the fact that notification of the breach of security is required under the Data Security and Breach Notification Act, intentionally and willfully conceals the fact of the breach of security, shall, in the event that the breach of security results in economic harm to any individual in the amount of $1,000 or more, be fined under this title, imprisoned for not more than 5 years, or both.

This proposed legislation may or may not become law. However, the simple fact that lawmakers are now discussing criminal charges for cases of public deception puts a very fine point on citizens' lack of tolerance to the same ole same ole.

WHAT IS REQUIRED? WHAT SHOULD YOU DO?

Organizations that store, process, or transmit data of value need to take serious stock of their security posture and think long and hard about two questions:

- What is presently required sufficient to establish a defensible position of reasonableness?
- More importantly, are you willing to wager five years of your freedom on it?

If you cannot answer "Yes" to either question with 100% certainty, you may want to adjust your expectations of what should be done.

Melinda R. Biancuzzo

Associate Attorney, Gibson, Dunn & Crutcher LLP

Melinda practices in government contracts and cybersecurity and data privacy. She advises clients on all aspects of cyber incident and data breach response, including working with forensic security consultants, conducting internal investigations, interacting with law enforcement, and complying with data breach notification laws.

SECURITY WITH EMPATHY: **HOW TO DELIVER SECURITY FINDINGS AND NOT BE HATED**

As security practitioners we are in the business of building the most secure systems that allow people to do what they want, within reason. Part of this mission is identifying problems in a system or process so the appropriate people can fix or mitigate them.

Here's the issue: The way you deliver security findings has a huge influence on how well your customers or colleagues fix the problem. If you do it well, they'll take the issues seriously and work out the best ways to implement what you've recommended. If you do it badly, even if you're 100% right, they'll hate you. Just think how you'd react if some smart-ass said you'd done something badly and now you had to do a whole lot more work to fix it.

Here are some ways I've learned to do my job as a pentester in a way that means the teams I report my findings to don't hate me.

DON'T EXAGGERATE FINDINGS

When I'm head down into testing a site, it's emotionally draining. I never know what I'm going to find. So when I find something that took hours or days to identify, I get excited and say to myself "This is a critical vulnerability.“

Pull back from this urge. Ask yourself, what's the worst that could happen with this vulnerability? How easy is it to exploit? Use this information to evaluate the real risk of this issue and make sure you reflect that in your findings.

DON'T BE CONDESCENDING

Security is hard. Security teams need dedication and organizational focus to continually make their environment more secure. It's a process and you are part of that process. Remember that security analysts or software developers are not stupid or ignorant. They're trying to accomplish a thousand things you don't know about. They have to balance delivering features or capabilities quickly against delivering them securely.

A perfectly secure product that never gets released never makes any sales; a poorly secured product gets eaten by wolves. Security is a journey and never a destination. The goal is to make the system more secure continually.

DON'T PUSH YOUR CUSTOMER UNDER A BUS

A lot of times the security team will hand your report to people in leadership roles. However, the people who commissioned you to do the pentest are the ones who will have to fix the issues and take responsibility for them. Use terms that help the security or development team maintain their reputation while their managers are reading the report.

Don't say "This security was not implemented properly." Try "Here are some better ways to implement this function." You probably don't appreciate all the concerns that your customer was trying to handle.

If you're pretty sure a bug is easy to fix, say so. Don't say "The character '&' was not handled properly and allowed exploitation." Instead say "The character '&' is incorrectly encoded but this is easily mitigated by properly encoding the '&' character."

If you see what they were going for in a feature, add that. Don't say "The password hash function is weak and vulnerable to brute force attacks." How about "This hash algorithm is not highly resistant to brute force attacks; a stronger algorithm would better protect against brute forcing."

IF THEY DID SOMETHING WELL, GIVE CREDIT

If your customer implemented a feature or system securely, say so. If they used a strong hashing algorithm or had components that resisted all your attacks, by all means include that in your report. One way I like to do it is to list the attacks I tried. "I tested for cross-site scripting, cross-site request forgery, and SQL injection. None of the attacks were successful. Good job!"

It helps show that you're not just out to get them. It also shows them that you're on their side and this is a goal we are trying to reach together.

SECURITY IS A JOURNEY

Remember that security is a journey. Never expect a product or environment to be completely secure; in my experience they never are. Instead, be a part of this system and deliver findings in a way that makes people more likely to take your concerns serious and fix them.

Shawn Lee

Cybersecurity Consultant, Application Security, Nuix

Shawn has built and designed many architectures that focus on privacy and protecting systems from misuse for numerous S&P 500 organizations. He designed and built the Nuix malware pipeline and he invented a patented technology that protects customers' personal information during the ecommerce checkout process.

IS IT TIME TO RETHINK AUTHENTICATION?

Everyone wants their private data to be secure but easily accessible. We know that personally identifiable, financial, and health data are valuable. However, most people's online behavior suggests they believe data security is not their problem but the responsibility of the organizations with which they transact.

Public trust in any organization is eroded when its supposedly secure digital or physical environments are breached, exposing private data. The cost to each individual might vary but it causes major reputational and financial loss for the breached organization.

Yet, many organizations appear to only take data protection measures as required by law, rather than focusing on removing actual breach risks. This "compliance versus security" stance is unacceptable. The best stance is to assume breaches will happen, and address the challenge now.

IMPROVING THE SECURITY OF PRIVATE DATA

The first step is to ensure your most valuable data is and locked with keys that can't be stolen or easily guessed.

The second step is to give individuals back control of their private data. Private data should no longer be visible on any network by anyone without the correct authorization from the individual owner. Even then, the data owner should have full control of how much of it can be unlocked, and how it will be used.

The third step is to separate authentication layers from the systems, servers, and applications they're protecting. This means ensuring access keys are not only strongly encrypted but no longer stored in their entirety in one place.

Traditional central authentication stores might be convenient for organizations but they are very attractive targets for hackers. Once hackers are inside a server holding these records, they know they can access a wealth of information, including the keys (such as usernames and passwords) to help unlock other systems and records.

And the oldest model of authentication—username and password—needs to be retired.

PASSWORDS ARE RISKY AND OUTDATED

The username and password method for controlling data access is already four (human) generations old. Back in the late 1950s, systems admins for MIT's Compatible Time Sharing System wanted to set up basic access controls for their mainframe computers. They mainly needed a record of who logged on and when so they took the library card model (username) and asked each user to store it with a unique signature or password in two locations:

1. The Compatible Time Sharing System's central authentication record; and
2. The user's own brain.

Of course, some people recorded passwords elsewhere, making them easier to remember, share, or steal. Back then access authentication—not security—was the priority.

These days, most systems rely on just one piece of the key: a password. The second piece (a username or email) is often publicly known or easily reverse-engineered.

Most people are nonchalant about passwords. They think it's a pain inventing and remembering long strings of letters, numbers, and symbols that make a password stronger. So they reuse a small collection of favorite passwords for email, business systems, social media, and payment gateways, making it easy for hackers to compromise multiple accounts. Or if they use a password manager on a device, they're not smart about securing access to the device itself.

Cybercriminals typically attack the weakest access point—whether that's a person, device, or gateway—aiming to steal credentials that could be used to compromise multiple accounts.

Using weak passwords, and reusing them, is extremely risky, though all kinds of people still do it:

- Facebook founder Mark Zuckerberg had his identity hacked in June 2016 because he'd reused a password across multiple systems.[1]
- Microsoft's 2017 Security Intelligence Report revealed a three-fold increase in user accounts attacked since 2016 and warned: "[most] of these ... are the result of weak, guessable passwords and poor password management."[2]

- Google's 2017 study into the risks of stolen credentials found 12 million users' credentials were stolen through email phishing and 3.3 billion credentials were compromised during third-party breaches.[3] "Passwords are no longer a paradigm that you can really trust in," warned Google anti-abuse researcher Kurt Thomas in a November 2017 interview with Mashable, adding that too many people disregard advice about not reusing passwords.[4]

WHAT ABOUT 2FA?

Many organizations implement multifactor authentication, in which the user provides some login information and the organization combines this with a secret (such as a biometric or a key to generate a one-time code) to unlock access. These systems make access more complicated for users and all those layers add up to extra costs.

> *"Public trust in any organization is eroded when its supposedly secure digital or physical environments are breached, exposing private data. The cost to each individual might vary but it causes major reputational and financial loss for the breached organization. Yet, many organizations appear to only take data protection measures as required by law, rather than focusing on removing actual breach risks. This "compliance versus security" stance is unacceptable. The best stance is to assume breaches will happen, and address the challenge now."*

The popular two-factor method of sending a unique code by email or text message relies on a broken and untrusted username (likely to be publicly known) and a mobile device (which may be stolen) or an email account (which may be compromised). The US National Institute of Standards and Technology requires agencies to consider the substantial risks of using text message authentication codes for services that plug into government IT systems.[5]

FUTUREPROOFING AUTHENTICATION

Modern password generation and data encryption technologies might offer some protection for now, as their codes take a long time to break with contemporary computers. But they're not invulnerable.

"The encryption schemes today are based on factoring and on prime numbers, so if you had a [quantum] computer that could factor instantly, if it did that today it could break all encryption schemes," said David Awshalom, an experimental physicist at the University of Chicago's Institute of Molecular Engineering.[6]

So, what steps can organizations take to prepare for when quantum computing takes off?

"Securing data will require protection against quantum algorithms, or a system of public and private keys that erase, renew and rotate themselves over time," explained journalist Meredith Rutland Bauer.[7] "This means that hackers would scrape data that would become useless in the future, because the keys necessary to access that information would have already self-destructed."

DECENTRALIZED AUTHENTICATION USING ROLLING KEYS

At Haventec our approach is to never store any user secret or private encryption key anywhere.

Each time we authenticate a user we identify the device and reconstruct the single-use private key mathematically. Once authenticated, we destroy all keys for that user. We immediately create new keys, deconstruct and distribute them, ready for the next authentication request.

This provides a much stronger mechanism than traditional two-factor authentication. It also protects against common attacks such as phishing, shoulder surfing, social engineering, password cracking and malware keylogging.

Maintaining privacy in every interaction helps you build trust. When that trust is mutual, you make it easier for people to do business with you.

Robert Morrish

CEO, Haventec

Robert Morrish is a seasoned technologist with more than 27 years' experience taking innovations from concept through to commercialisation. Robert joined Haventec in March 2016 from Macquarie Group, where, he was instrumental in transforming Macquarie's digital API platforms. He was previously involved in two other successful Australian start-ups: Sabela Media and Decide Interactive.

[1] *Robert McMillan, Mark Zuckerberg's Twitter and Pinterest Accounts Hacked, Wall Street Journal, June 7, 2016*

[2] *Microsoft, Security Intelligence Report volume 22, March 2017*

[3] *Kurt Thomas et al, Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials, November 2017*

[4] *Mark Kaufman, After a year of intensely investigating password theft, here's what Google found, Mashable, November 14, 2017*

[5] *Paul Grassi et al, NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management, National Institute of Standards and Technology, June 2017*

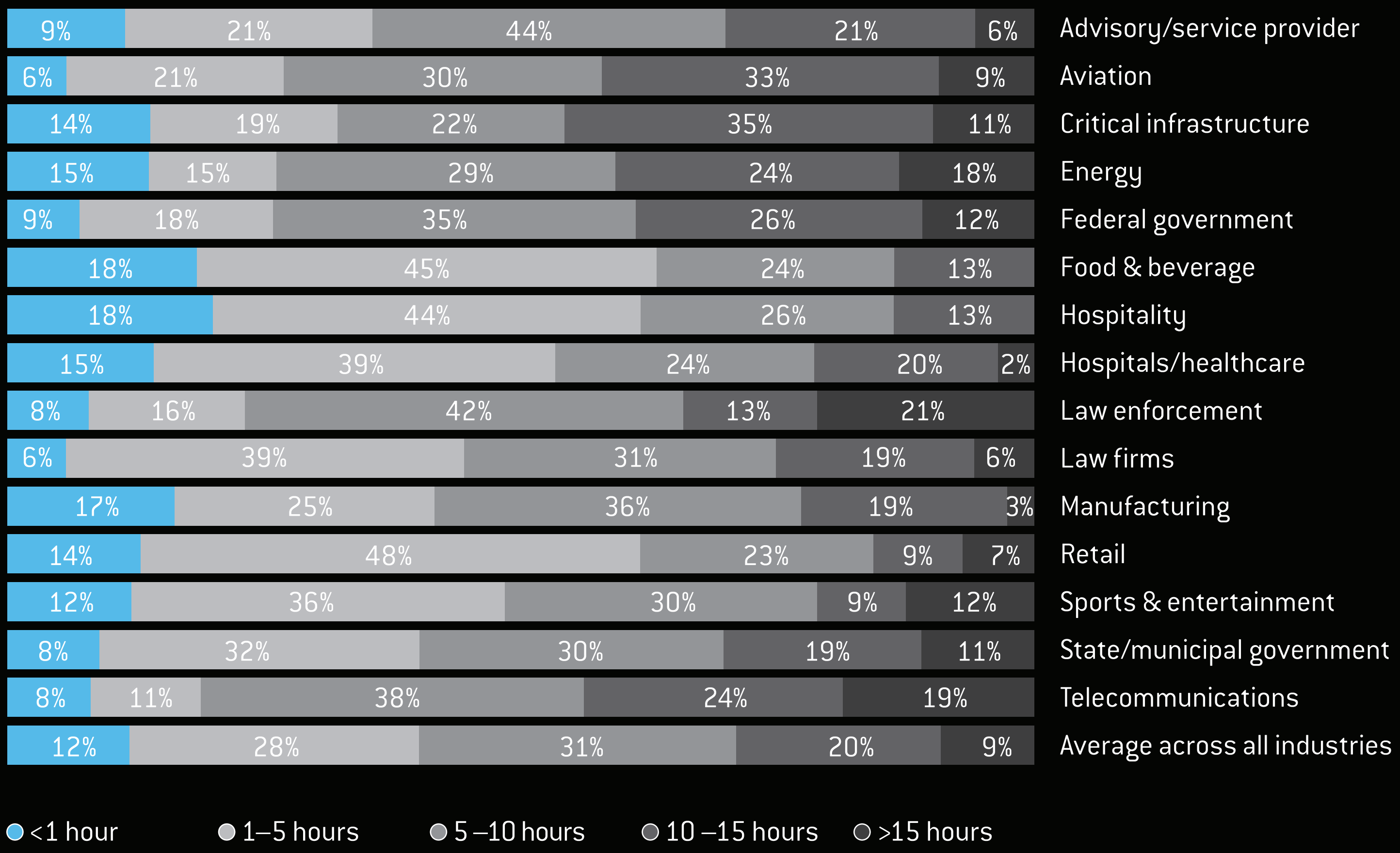
[6] *Jeff McMahon, Will Quantum Encryption Arrive Before Quantum Computers Break All Our Passwords?, Forbes, April 17, 2016*

[7] *Meredith Rutland Bauer, Quantum Computing Is Coming for Your Data, Wired, July 19, 2017*

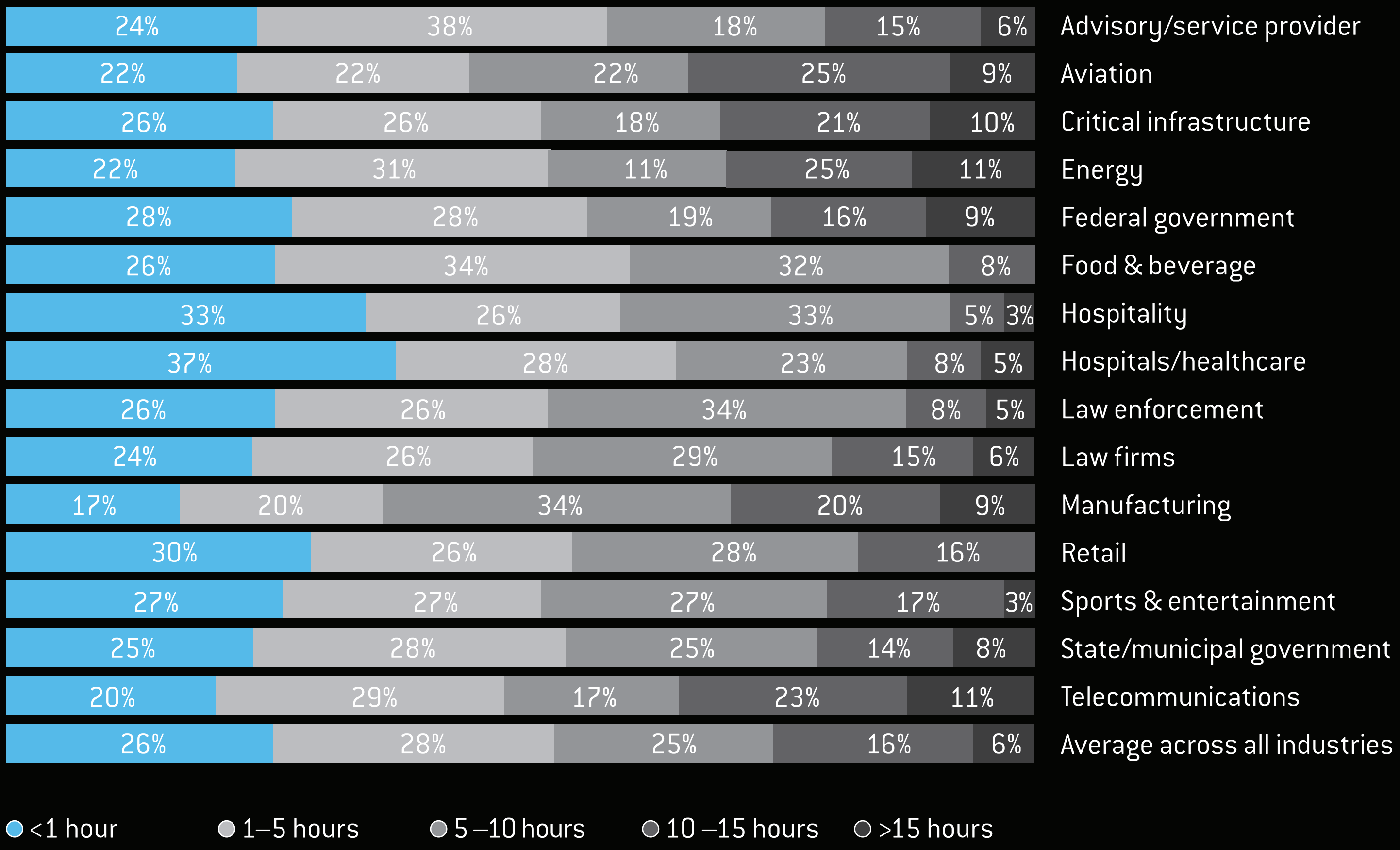
08

APPENDIX A: BREACH BREAKDOWN BY INDUSTRY

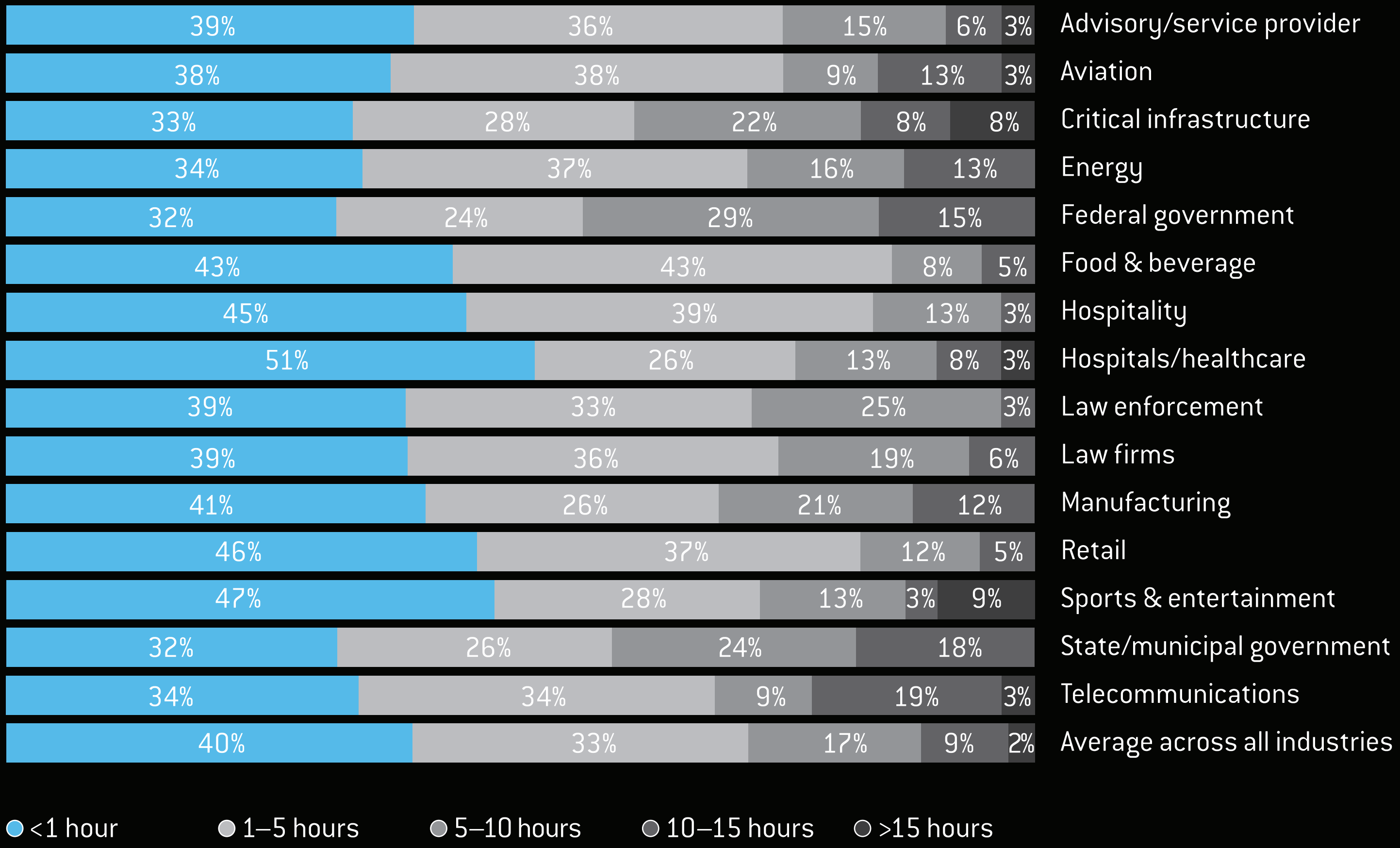
HOW LONG ON AVERAGE DOES IT TAKE YOU TO BREACH THE PERIMETER OF YOUR TARGET?



HOW LONG ON AVERAGE DOES IT TAKE YOU TO IDENTIFY CRITICAL VALUE DATA AFTER BREACHING THE PERIMETER?



ONCE YOU HAVE IDENTIFIED CRITICAL VALUE DATA, HOW LONG DOES IT TAKE TO EXFILTRATE THAT DATA?



09

THE FINAL WORD: **OFFENSE IN DEPTH**

Information security experts understand the strategic value of practicing defense in depth. The concept is straightforward: apply a multi-layered defense toward an organization's information resources. This approach yields two powerful benefits: it ensures security coverage (or at least consideration) from a holistic perspective and it provides the benefit that one defensive mechanism may save the day when another fails.

MULTIFACETED DEFENSE

The concept of a multifaceted defensive strategy has been around for generations in the physical world. The United States Secret Service's approach toward physical security is a good example. When the Secret Service prepares a location for a presidential visit, it does not just rely on the agents who stand next to the president. It deploys canine patrols, metal detectors, fences and barricades, patrol helicopters, rooftop counter-snipers, and rings of uniformed and plain-clothes officers. Even if one area of defense fails, it will be mitigated by other defensive layers.

Unfortunately, criminals often deploy the same strategy. Think of how many ways someone can steal money from you: they can rob you on the street, break into your house, scam you, blackmail you, hack into your bank account, or compromise your credit card.

> *"Organized crime groups have adroitly shifted from one criminal activity to another—bootlegging, prostitution, illegal gambling, narcotics, political corruption—based on profitability, convenience, and other factors. Now online enterprises are part of the organized crime smorgasbord."*

This sort of "offense in depth" has plagued law-abiding people for centuries. Organized crime groups have adroitly shifted from one criminal activity to another—bootlegging, prostitution, illegal gambling, narcotics, political corruption—based on profitability, convenience, and other factors. Now online enterprises are part of the organized crime smorgasbord.

MULTIFACETED ATTACK, TOO

Some well-known hackers have demonstrated their mastery of a multifaceted approach. Albert Gonzalez, who ran a far-reaching and profitable hacking crew, moved skillfully from one method to another based on increased profitability and decreased risk. His group began with wardriving, moved into point of sale hacking, then learned to excel at SQL injection attacks. Gonzalez was an enterprising criminal who constantly searched for the next big thing, a new (or newer) method of hacking that would bring in more money, faster, and with less risk of getting caught.

We may never know exactly how many offensive cyberattack techniques exist but we know the supply is plentiful and constantly growing. The famous book Hacking Exposed by George Kurtz, Joel Scambray, and Stuart McClure has twelve chapters, each describing multiple attack methods—and the latest edition is five years old! The EC Council's Certified Ethical Hacking certification program covers 18 separate modules, each focusing on a specific hacking category. Online criminals clearly have a well-stocked arsenal at their disposal.

GET INTO THE MINDS OF HACKERS

The 2018 Nuix Black Report provides a unique and sober verification of the techniques available to hackers and penetration testers. There are plenty of annual data breach studies that analyze after-action reports from law enforcement and victims. But while these reports provide useful information about the methods of attacks, only the Nuix Black Report provides the hacker's perspective. The unique data gathered by the Nuix Black Report includes fascinating information such as average length of time it takes to breach a network, the industries that are easiest to hack, which defensive mechanisms provide the least value, and which offensive measures are most effective.

The Nuix Black Report confirms that hackers utilize their copious supply of weapons, including private exploits, exploit packs, commercial tools, open source tools, and custom tools. Social engineering, in its various forms, is always a favorite option. This valuable insight into the attack mindset demonstrates that a defense-in-depth security approach has never been more important.

IT WILL HAPPEN TO YOU

The most valuable lesson from the 2018 Nuix Black Report is that no industry is safe. What is more dangerous than thinking "it won't happen to me" is thinking "nobody would want to hack me." I promise you, somebody does.

If you want to keep your organization from appearing in Krebs on Security, or protect your personal devices from joining the next botnet, learn the important lessons from the Nuix Black Report and strengthen your defense-in-depth strategy.

David Smith

Chief Information Security Officer

David is responsible for Nuix's internal information, physical, and personnel security programs. He served in federal law enforcement for 27 years, including 24 years as a Special Agent for the United States Secret Service. David is a federally certified instructor with over 3,000 teaching hours in forensics and cybercrime.

ABOUT NUIX

Nuix understands the DNA of data at enormous scale. Our software pinpoints the critical information organizations need to anticipate, detect and act on cybersecurity, risk and compliance threats. Our intuitive platform identifies hidden connections between people, objects, locations and events—providing real-time clarity, control, and efficiency to uncover the key facts and their context. **www.nuix.com**.

NORTH AMERICA
USA: +1 877 470 6849

EMEA
UK: +44 203 934 1600

APAC
Australia: +61 2 9280 0699