
nuix
THE
BLACK
REPORT
DECODING THE MINDS OF HACKERS

THE BLACK REPORT 2017

CONTENTS

Lead author: *Chris Pogue*

Editor: *Josh Mehlman*

Designers: *Stephen Burnett, Jon Chamot, Grant Whitehouse*

Production manager: *Chantelle Sagurit*

Contributors: *Chris Brewer, Stuart Clarke, Ale Espinosa, Dr. Claire Ferguson, Dr. Jim Kent, Grayson Lenik, Alexander Major, Evan Oslick, Andrew Spangler, Chief Terry L. Sult, Corey Tomlinson, Melissa K. Ventrone, Aleksandra M. S. Vold*

Figures in charts may not add up to 100% due to rounding.

KEY FINDINGS

81%
of the hackers we interviewed said they could identify and exfiltrate your data in less than 12 hours.

88%
of respondents claimed they could compromise a target in less than 12 hours.

75%
of the time, organizations only conduct limited remediation after a penetration test, usually focused on critical and high vulnerabilities.

50%
of respondents changed their attack methodologies with every target.

84%
of respondents used social engineering as part of their attack strategy.

69%
of respondents reported that security teams almost never caught them in the act.

42%
believed data hygiene and information governance were the least impactful use of security dollars.

52%
said employee education was an extremely important countermeasure.

76%
of respondents spent 1 – 10 hours per week researching security news and technology.

64%
said their biggest frustration was that organizations didn't fix the things they knew were broken.

100%
of hackers, pentesters, and forensics experts agreed that once someone has accessed your data, it's gone — like gone gone.

76%
of respondents believed technical certifications were not a good indication of technical ability.

NOT ANOTHER CYBERSECURITY REPORT

There's no shortage of research reports about cybersecurity. A web search for the term "cybersecurity reports" yielded 11.5 million results; the top hits included such familiar names as Mandiant–FireEye, Dell, IBM, AT&T, Cisco, Google, Microsoft, ISACA, Verizon, Symantec, Trustwave, and Force Point.

With so many of the biggest names in the industry publishing reports, how can yet another report provide additional value or insight? How can it avoid being white noise?

Let's suppose that new report was fundamentally different than the rest; it reported new information from a unique perspective in a way that showed being different would actually make a difference. That's a report I'd like to read.

The Template for a Generic Cybersecurity Report

During my tenure in the cybersecurity space, I have read literally hundreds of threat reports that all seemed to report the same thing. While there were variations in the data samples upon which the reports based their findings and conclusions, the overall messaging remained constant:

- Attacks are happening all over the world
- Attacks are growing in frequency across all target verticals
- No data is safe
- Organizations are failing to prevent or detect attacks in any sort of meaningful way
- Governments all over the world are looking to introduce legislation to compel the private sector to increase its security posture.

Delivering the Wrong Message?

There is clearly value in providing measurable statistics that security professionals can use to communicate the gravity of the challenges they face to executive decision makers and boards of directors. These reports lend credence to the difficult messages that they need to deliver and that the business needs to understand: This is not a game, the threat is real, and we either take preventative measures now or (much more difficult and expensive) reactive measures later. But are those messages telling the right story in the right way to the target audience?

If these messages were having a net positive effect, surely we would see some improvement in our current situation. Yet, year after year, we learn that offensive capabilities have far outpaced defensive capabilities; data breaches are more frequent; and attacks are growing increasingly complicated. Detection and response are critically important, yet only marginally effective. So it would seem the industry's approach to cybersecurity over the past two decades leaves something to be desired.

Countless security vendors and solution providers have claimed their widgets were all you needed to prevent attacks and if you would only buy this feature or that add-on, your organization would be practically un-hackable. Well, we all bought their solutions, deployed them within our environments, and expected to be safe; yet we were still compromised. So there is obviously something to this problem beyond what we have been led to believe that continues to plague virtually every organization on the planet.

Ask the Attackers

This is why I feel comfortable in asserting that the data and insights contained within the Nuix Black Report are going to make a difference. We've avoided compiling data about incidents that have already taken place or highlighting trends and patterns in data breaches—these are clearly the symptoms of a deeper problem and honestly, more of the same is unnecessary. Instead, we have focused on the source of the threat landscape: the attackers themselves.

During Black Hat USA and DEFCON 24 in 2016, we conducted a survey of known hackers, professionally known as penetration testers, and asked about their attack methodologies, favorite exploits, and what defensive countermeasures they found to be the most and least effective—and many other questions. One individual told me, "The only difference between me and a terrorist is a piece of paper [a statement of work] making what I do legal. The attacks, the tools, the methodology; it's all the same. Besides … I'm far too pretty to be in jail."

A Unique Perspective

Rather than relaying what was taking place, this research gave us hard data on how it was happening. We could draw a clear correlation between which security countermeasures had an impact and which did not—not based on the opinions of executives or security directors, but on what the hackers were telling us first hand. This is an entirely different perspective on the threat landscape; instead of hearing from the victims, we're hearing from the attackers.

What we found during our research was quite contrary to the conventional understanding of cybersecurity. Some countermeasures that you think will stop an attacker won't even slow them down. Other defensive techniques that you think are totally arbitrary actually have a tremendous impact on your defensive posture. We found that unequivocally, perception and reality are in desperate need of realignment.

Find Out What Works

The data and articles contained in this report will illuminate the true nexus between attacker methodology and defensive posture; showing you which countermeasures will improve your security posture and which are a waste of money and resources. You will learn what is the best spend for your security dollar and, more critically, why.

I am thrilled to be a part of such a unique and desperately needed body of work. We are shining a light on the darkest recesses of the threat landscape and uncovering the driving forces behind what has been referred to by many as the greatest threat the global economy has ever faced.

No more guessing. No more wondering. No more hoping.

Welcome to the Nuix Black Report.

Chris Pogue — Chief Information Security Officer, Nuix

Chris is Nuix's Chief Information Security Officer and head of the Cyber Threat Analysis Team. He is responsible for Nuix's internal cybersecurity measures and manages the company's security services organization. His extensive experience is drawn from careers as a cybercrimes investigator, ethical hacker, military officer, and law enforcement and military instructor.

WHO ARE HACKERS?

A layperson's view of a professional penetration tester (pentester) likely does not align very well with reality. The stereotypical image is of dark basements dimly lit by the soft glow of flat screen monitors; with pizza boxes, soda cans, and candy wrappers overflowing from a metal trash can and littering the floor around it. Thrasher or Goth music is rhythmically juxtaposed against the steady, rapid tap tap tap of fingers across a keyboard. The guys (and they're all male) are brooding, hooded, and singularly focused on stealing data; the modern day equivalent of contract hitmen.

More realistically, pentesters are regular guys and gals wearing jeans and chucks. They're just as likely to listen to Journey, Bruno Mars, or Pharrell as Bauhaus or the Cure. Like many other people in the information technology world, they're just working hard to make a living. Most have very nice homes that are well lit, trash free, and well … probably lit more by computer screens than other light sources. When I was hacking all the things, I preferred the Beastie Boys and the Clash to Suicidal Tendencies—although Skittles and Mountain Dew were among my five top food groups.

For the purposes of this report however, we are far more interested in what these professionals think of themselves, the world around them, and the cybersecurity landscape.

View of Self

Based on the survey results, 53% of respondents saw themselves as a combination of hackers, professional pentesters, and students of technology.

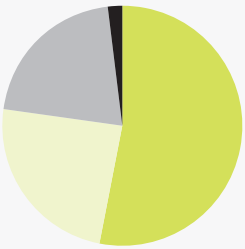
- 24% saw themselves primarily as students of technology.
- 21% saw themselves as specifically professional pentesters.
- Only 1% called themselves full-time hackers.

A wise person once told me if you love what you do, you'll never work another day for the rest of your life. This is true for many of our respondents; they clearly love technology and security and are truly passionate about their craft. Among security practitioners, the "Chihuahua on the pork chop" mentality (as my friend Cindy Murphy calls it) seems to be the rule rather than the exception. Our survey found that two-thirds of respondents enjoyed hacking because they liked the challenge. Another 31% said they were in it for the money and only 3% did it for ideological reasons.

Pentesters have a unique perspective on the legality of their activities since fundamentally what they are doing constitutes criminal activity or terrorism in just about every country in the world … unless they have proper authorization in the form of an indemnity letter or statement of work.

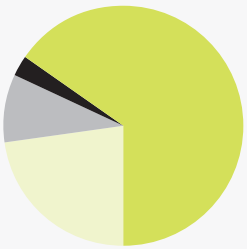
Nearly two-thirds (64%) of respondents believed there was more to something being "right" or "wrong" than what a government had decided to legislate. Unexpectedly, 28% showed no sign of sympathy for hackers who were arrested for their activities. Only 7% felt that those who were arrested were likely victims of circumstance, and only 2% indicated "that the targets of data breaches had got what was coming to them."

How would you categorize yourself?



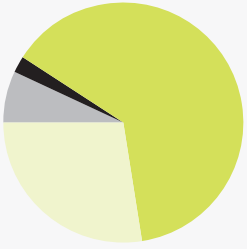
- I'm a mix of all the above; it depends on the circumstances 53%
- I'm a student of technology; I hack to learn 24%
- I'm a professional penetration tester; I don't touch anything without an indemnity letter 21%
- I'm a full-on hacker; laws are arbitrary to me 1%

What is your main motivation as a hacker/pentester?



- I like the challenge 66%
- I like to "smash the stack for fun and profit" 23%
- I'm all about the Benjamins! $$$ 9%
- I'm an ideologue and in it for "the cause" 3%

When I read about hackers being arrested and convicted, my response is usually…



- "Legal" is a myopic way of looking at it; there is more to "right" and "wrong" than what the government decides to legislate 64%
- Serves them right; hacking without an indemnity letter is illegal! 28%
- This is nonsense; these guys are victims of circumstance 7%
- Some corporations deserve to get hacked; these guys are just doing what's right 2%

Education Level

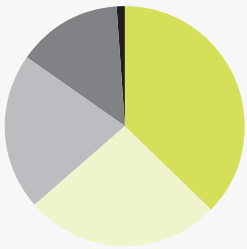
Another significant departure from popular belief is in education; the hacking community is far more educated than many people believe. Around two in five respondents (37%) had a college degree and just over one quarter (26%) held advanced degrees. Another 21% had only a high school education, 14% saw limited value in formal education, and a meagre 1% had General Education Development (GED) degrees.

This is not to say many people go to college to become hackers or pentesters; in fact, there are very few practical cybersecurity courses anywhere in the world. I believe many people end up becoming hackers because so many countries have strong tertiary mathematics and computer science programs, provided free of charge or greatly discounted, but have weak technology job markets. When these students graduate, they can either look for work outside their country, try to find a local job for what is likely a marginal salary, or work for a cybercrime group—or as professional hackers—making considerably more money and contributing to their local economy.

In addition to formal degrees, two-thirds of respondents held between one and three technical certifications and one-fifth (20%) had between three and five. Only 6% had between five and seven certs, 4% have between seven and 10, and 4% have 10 or more.

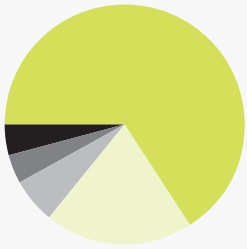
More than three-quarters (76%) of respondents felt that technical certifications were not a good indication of technical ability. This finding is interesting because job applicants need a mechanism for distinguishing themselves from their peers. In other words, many respondents did not consider technical certifications a way to communicate their knowledge as much as a way to get their foot in the door for job interviews—it's about playing the "HR game"

What is your highest level of education?



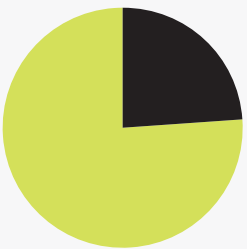
- College graduate 37%
- Postgraduate degree 26%
- High school graduate 21%
- Formal education is for suckers 14%
- GED 1%

How many technical certifications do you have?



- Less than three 66%
- 3–5 20%
- 5–7 6%
- 7–10 4%
- More than 10 4%

Do you believe technical certifications are a good indicator of technical ability?

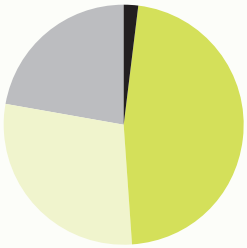


- Yes 24%
- No 76%

and getting past filters (something hackers are usually good at anyway). In this sense, certifications are more of a necessary evil than a measure of technical ability.

As for informal education, almost half (47%) of respondents spend between one and five hours per week keeping up with the latest developments in the industry. Only 2% spend less than an hour and 22% spend more than 10 hours each week reading security news, listening to podcasts, and broadening their knowledge. Clearly, maintaining a current understanding of the dynamic technologies landscape is tremendously important to these security professionals.

How much time per week do you spend keeping up with the latest security news and technologies?



- 1–5 hours 47%
- Over 10 hours 22%
- 6–10 hours 29%
- Less than an hour 2%

Professional Employment

Professional pentesters work for companies of every size, from being self-employed, to working for very large companies with more than 50,000 employees. The relatively even distribution of results, save the 29% outlier, shows that our respondents color our data with a well-represented diversity of employment backgrounds.

What type of organization do you work for?

- Medium-sized business (500–4,999 people) 29%
- Very large business (more than 50,000 people) 19%
- I'm self-employed 16%
- Small-ish business (20–499 people) 13%
- Large business (5,000–49,999 people) 13%
- Small consultancy (less than 20 people) 11%

Most respondents spent a considerable amount of time bypassing security systems in a given 40-hour week. Just over half (51%) spend one-third to half of their time per week actively bypassing security and a workaholic 13% of them are at it more than 50 hours each week. When we remember that 76% of those we surveyed spend from 5–10 hours per week researching security news and technology, we found that the largest number of respondents spend between half and three quarters of a 40-hour work week actively hacking or researching how to hack.

Approximately how many hours a week do you spend bypassing IT security systems?

- 0–10 29%
- 21–30 15%
- 41–50 10%
- 10–20 22%
- Over 50 13%
- 31–40 10%

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 popularity. 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, there may still be one of several different reasons or motives behind the behavior, including:

- Monetary gain
- 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.

---

[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

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 hacking a particular 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.

---

[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

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.

Most relevant to hacking behavior seems to be Hirschi's notions of attachment, commitment, and belief.[10] 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 offence. This theory is helpful for understanding hacking behavior motivated by status, cause, and justification.

Understanding the Elements of Cybercrime

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. This being the case, these theories are useful in determining the bio-psycho-social elements of these offences, which can inform crime prevention strategies or at least provide a clearer understanding of the elements motivating these types of offences.

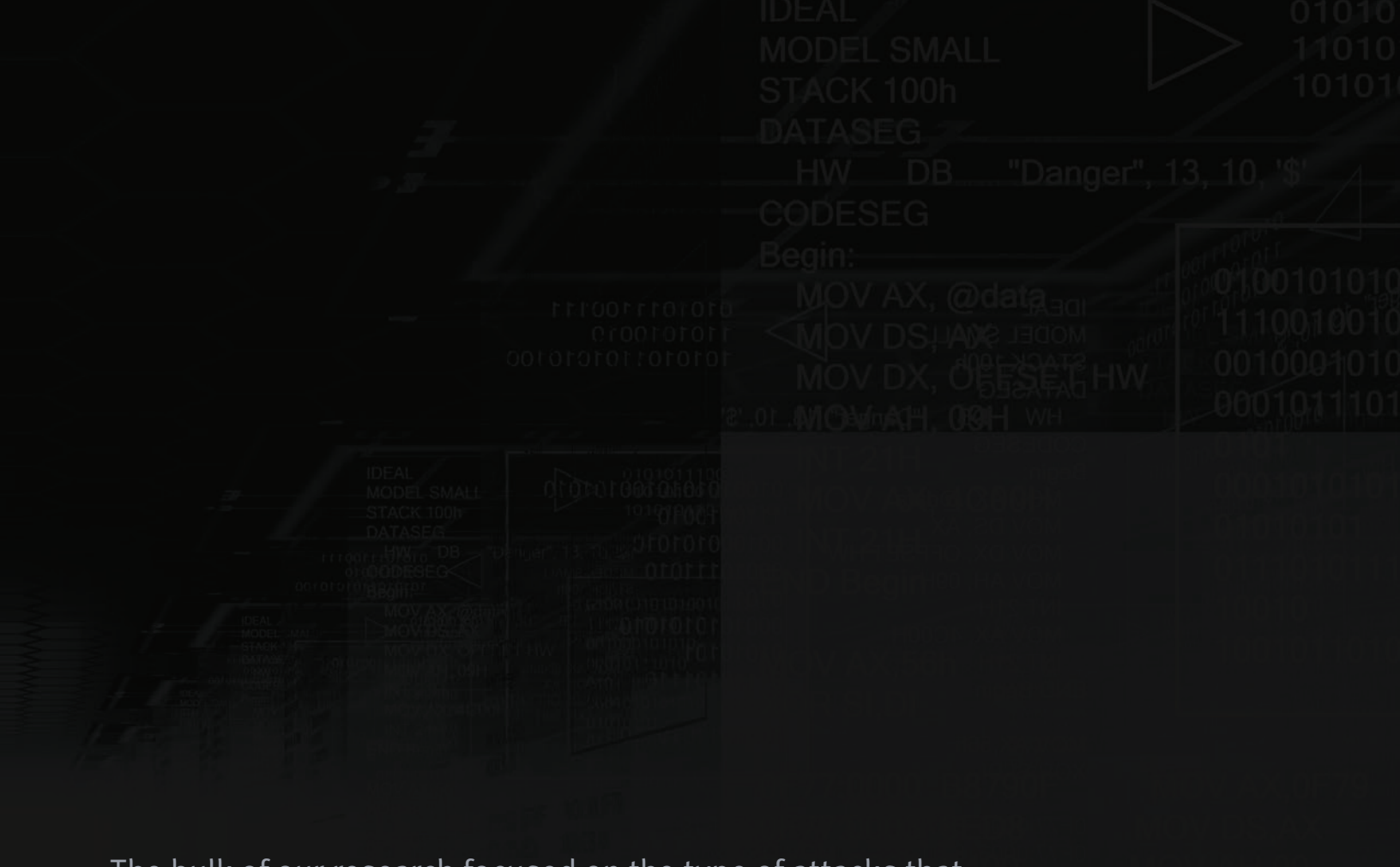
[9] Travis Hirschi. Causes of Delinquency. Berkeley: University of California Press, 1969

[10] Young & Zhang, Op. Cit.

Dr. Claire Ferguson – Lecturer, School of Justice, 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.


WHAT DO
HACKERS
KNOW?



The bulk of our research focused on the type of attacks that professional hackers carry out. We wanted to understand which techniques were the most effective, which security countermeasures actually prevented breaches, and how frequently respondents' clients identified their presence during an attack.

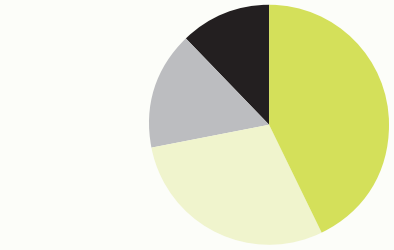
We believe this information provides critical insight for defenders. Many security vendors focus on their customers—the people who write the checks—rather than on the people whose job it is to circumvent the security controls they are trying to sell. While this makes sense from a marketing perspective, it's a terrible idea for security.

The survey results in this section should help realign your understanding of where your organization's security dollars are best spent and how likely your security programs are to succeed.

Most Successful Attack Methods

During the reconnaissance stage of an attack, 84% of pentesters use some aspect of social engineering to gather information about their targets. Only 16% claimed they never used this attack method.

How often do you use social engineering to obtain information about a target?

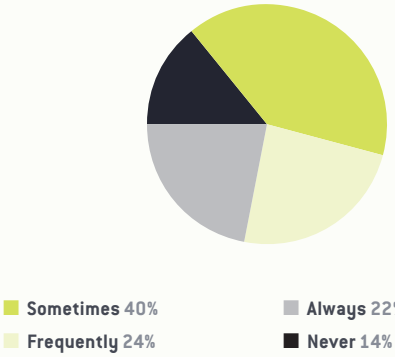


Sometimes 43%
Often 29%
Never 16%
Always 12%

It's important to point out that no security controls can fully mitigate or prevent social engineering attacks. That's probably why most pentesters use this vector to gather data about their targets. The only reliable way to prepare for social engineering attacks is to educate your staff about what these attacks are, how they are carried out and why, and what each individual can do if they suspect they are being attacked.

During the next stage of reconnaissance, 86% of hackers used vulnerability scanning to identify potential vulnerabilities in their targets; 24% said they did it frequently and 22% said they always did it. It's important to note that vulnerability scanning is only a part of the testing process—a scan on its own is no substitute for a comprehensive penetration test.

Do you use vulnerability scanning to identify potential vulnerabilities?

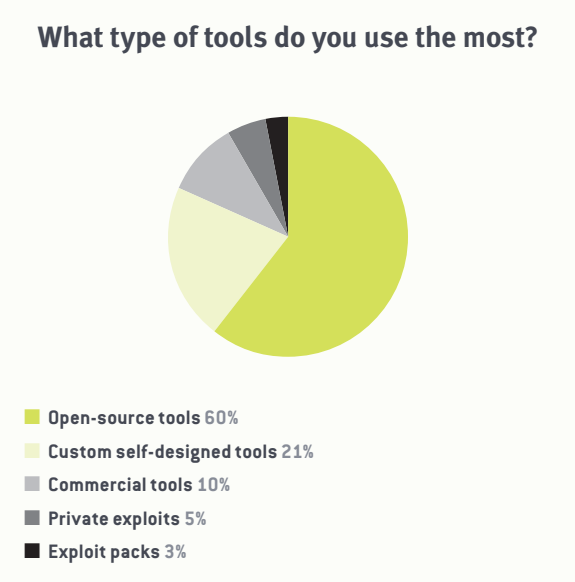


Sometimes 40%
Frequently 24%
Always 22%
Never 14%

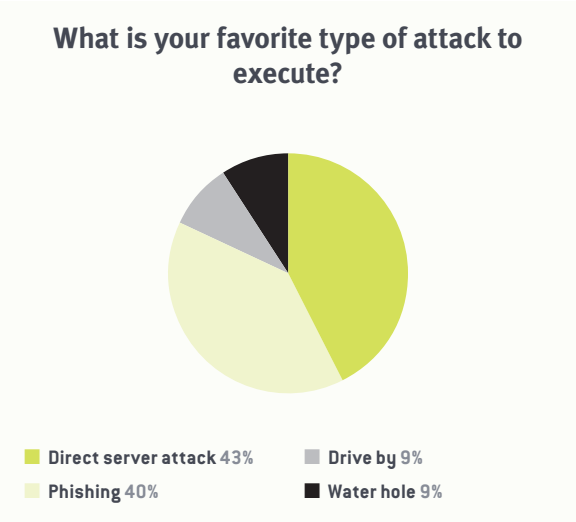
If security decision makers think attackers use commercial tools or private exploit kits to carry out their attacks, our data indicates otherwise. Only 10% used a commercial tool set such as the Core IMPACT exploit framework or the Cobalt Strike threat emulation package. An even smaller number owned up to using private exploit kits (5%) or exploit packs (3%). These are kits designed for often questionable or illegal uses such as infecting systems to make them part of a botnet or deploy ransomware. They may be available from little-known websites or forums (commonly called the "Dark Web") and at times specific exploit kits have contributed to a large proportion of compromises worldwide.

Instead, a large majority of respondents used open source tools (60%) or created their own custom tools (21%). This shows that the tools required to hack are easily acquired without having to pay large fees or frequent suspect websites. The majority of attacks organizations will face are generated using

non-commercial tools that are readily available to anyone with an internet connection. While pentesting and hacking require a lot of knowledge and specific skills, acquiring the tools is not a barrier to entry—anyone can get them and learn on their own how to use them.



Direct server attacks were the most popular method for breaking into systems, favored by 43% of attackers. Phishing attacks were also popular at 40%, while drive-by and watering-hole attacks came in at roughly 9% each. The relative popularity of direct server attacks shows that this vector is successful often enough to make it the most popular. Client-side attacks such as phishing are also popular because they are an effective way to circumvent the target organization's security controls without all the effort.



Time to Compromise

As defenders, you have precious little time to figure out what is going on during an attack. More than four in five respondents (88%) claimed they could compromise a target in under 12 hours; 28% took between six and 12 hours and an astonishing 43% found a way in within six hours. A frightening 17% of respondents claimed they could compromise a system in less than two hours.

If you cannot identify and stop an intrusion attempt in less than 12 hours, in all likelihood, at least one host will almost certainly be compromised. Realistically, you probably won't even have a sufficient understanding of the attack in two hours, much less be able to mount any sort of defense.

These numbers underscore the importance of having a well-trained response team using cutting edge technology actively monitoring for threats.

On average, how long do you estimate it takes you to compromise a target environment?

- 2–6 hours 43%
- 6–12 hours 28%
- 0–2 hours 17%
- More than 12 hours 12%

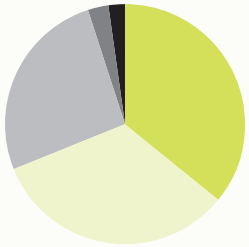
Despite the speed at which compromises take place, there are times when hackers run into systems they cannot break into. According to our study 53% of our respondents indicated that this happened sometimes (16% to 40% of the time), and 22% said that it rarely happened (6% to 15%). Only 16% said it happened often (41% to 100% of the time).

How often do you encounter systems you can't break into?

- Sometimes (16–40%) 53%
- Rarely (6–15%) 22%
- Often (41–100%) 16%
- Never (0–5%) 9%

Around one-third of the hackers we surveyed claimed their clients never caught them breaking into the target environment. A further 36% said they were caught around a third of the time by security teams while 26% claimed they were caught only half the time. A very small 3% lamented that they were almost always caught … I guess these guys have some work to do on their subterfuge skills.

Once you have compromised a target, how often does your target's security team identify your presence?



- Around a third of the time 36%
- Never, I'm a master of stealth and shadows 33%
- Maybe half of the time 26%
- I must suck at this, 'cuz I always get caught 3%
- More than half of the time 2%

Four-fifths (81%) of the hackers we interviewed said once they were inside the target systems, they could identify and exfiltrate the target data in under 12 hours; 31% said it took them between six and 12 hours, 29% got the job done in two to six hours, and 21% claimed it took them less than two hours.

Now, combine these figures with the finding that 88% of professional hackers can breach your perimeter in less than 12 hours, and you have a very important finding. In the first 24 hours of an attack, it is more than likely an attacker will compromise your systems, find and exfiltrate your sensitive data, and leave you none the wiser that they were ever there.

If this is the case, your organization had better have strong threat identification and response capabilities. Tick tick tick …

How long on average do you estimate it takes for you to find and exfiltrate targeted data after your initial breach?

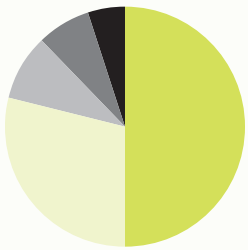
- 6–12 hours 31%
- 2–6 hours 29%
- 0–2 hours 21%
- More than 12 hours 19%

Changing Methodologies

Exactly 50% of our respondents changed their attack methodologies with every target. A further 38% changed things at least every six months. The smallest grouping (5%) said they changed things every 12 months or more … maybe these are the same people who keep getting caught?

Think about that for a second in terms of how most organizations defend themselves. Most defensive countermeasures focus on indicators of compromise (IOCs); these are known specific activities or programs that are associated with an attack pattern. Now, that would be an effective strategy if attack patterns either never changed, or only changed some of the time. However, according to our survey, 80% of respondents changed at least once every six months, often more frequently than that. How often do your IOCs change?

How often do you change your attack methodologies?

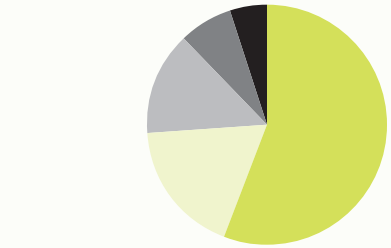


- Every engagement 50%
- 2–6 months 29%
- 1–2 months 9%
- 6–12 months 7%
- 12+ months 5%

The reasons for these changes were very interesting. A majority (56%) said it was to learn new techniques. Curiously, only 5% of respondents said they changed tactics because the old methodologies were no longer effective.

Both these findings indicate that if your defensive countermeasures are less flexible than the people trying to get around them, they have little to no chance of being effective; you will be protecting against an attack pattern that is no longer relevant. This underscores the importance of incorporating realistic, goal-oriented penetration testing into your security program. Only by continuously evaluating and enhancing your security countermeasures can you follow constantly shifting attack strategies.

What is the most common reason you change your attack methodologies?



- To learn new techniques 56%
- To reduce noise 18%
- Other 14%
- To improve speed 7%
- They no longer work 5%

RECOGNIZING AND REACTING TO TODAY'S SECURITY CHALLENGES

Before I joined Nuix, I worked as a security practitioner and experienced many of the challenges unveiled by our research for this report. What I saw here was a detailed and accurate reflection of what I already knew firsthand: The challenges of cybersecurity extend beyond technology; have implications for businesses small, medium, and large; and require something of everyone from frontline analysts to executives and directors.

These challenges, coincidentally, played a large role in bringing me to Nuix. In Nuix I saw an opportunity to build solutions to address many of the obstacles we've all faced for years.

Confronting the Skills Shortage

It's not news that there's a skills shortage in security and intelligence. One report speculates that there will be up to two million unfilled cybersecurity jobs by the year 2019.[1] This is especially interesting in the context of the attitudes toward education and certifications exhibited by the respondents to our research—all of whom are experienced and qualified in some way as cybersecurity professionals.

More than 60% of respondents were educated at a college level or above and about 35% held three or more technical certifications. Nonetheless, a vast majority of them believe that education holds little value. Over 75% did not believe technical certifications were an accurate indicator of ability.

We can only infer, then, that mastery and autonomy are key motivators for industry practitioners and that real-world experience trumps classroom learning and formal certification.

This is not good news if we think about the anticipated shortage of qualified professionals. Getting a job in cybersecurity is a lot like the classic conundrum that young people face when they want to buy a house or a car. Lending companies tell them "You don't have a credit history." They ask "How do you get a credit history?" Lenders say "By getting a loan and paying it off on time, every month." They respond "But you won't give me a loan because I don't have a credit history."

Similarly, cybersecurity rookies who have formal education or certification face an environment that is ambivalent to, or in some cases even hostile toward, a piece of paper that says they know what they're doing.

Is there a way that we can lower the bar and give them the opportunity to gain that experience, while at the same time giving veteran security practitioners the tools and information they need to do what they do more effectively?

Paving a New Path

The first step is to acknowledge the challenges we face. Next, we need to harness the myriad skills we have at our disposal to facilitate the development

[1] Kelly Sheridan, Cyber-Security Skills Shortage Leaves Companies Vulnerable, *InformationWeek*, August 1, 2016

of rich intelligence repositories, make data more accessible, and support collaboration to empower practitioners of all skill levels.

This approach admittedly represents a paradigm shift in the way that organizations approach building their cybersecurity teams. The framework behind Nuix's Security & Intelligence development is a prime example of a better way to look at evidence and make it easier and more efficient to work with.

Our people, objects, locations, and events (POLE) framework is intended to encourage and facilitate consistent and repeatable intelligence sharing across all kinds of organizations and between people with all kinds of skill levels. This framework also helps humanize data.

Why is this important? More than one-third (36%) of respondents said endpoint security was the most challenging countermeasure to overcome. Endpoint security solutions generate a lot of data. Your laptop or mobile device is a clear window into your digital habits but, unfortunately, that data is cryptic, unhelpful, and simply overwhelming to inexperienced security practitioners.

The idea of humanizing this data—of distilling it down to its POLE elements to tell a real story—is a critical component of preventing and investigating security incidents. It gives us the best possible chance of understanding the human and technical elements of an incident. And it becomes even more powerful when we include data from multiple intelligence sources—other endpoints, open-source repositories, or forensic artifacts—to enrich the picture.

Bridging Another Gap—What Do We Do Next?

Almost two-thirds (65%) of respondents' biggest frustration was that most organizations did not fix vulnerabilities after they were identified. I can think of many reasons why this might be the case: Money and time are at the top of that list. How can we, as an industry, improve on this in the future?

I believe strongly in the power of intelligence, even in this scenario.

Decision makers typically receive a vulnerability report and are told "This is broken and needs to be fixed." Often, these reports lack the intelligence or proper context that would help them make an informed, rather than visceral, response. What would you do if someone told you "This is bad for us if we don't fix it" with no further information?

To stand a better chance of protecting our data, we must harness and grow what we know by adopting a consistent framework for sharing and using intelligence.

Building Actionable Intelligence

Our research shows support for investing in preventative solutions, but the ongoing stream of data breaches demonstrates that attackers remain ahead of the curve. It's not hard to understand why. Over 70% of respondents to this survey said they spent more than 11 hours a week bypassing security. On top of that, 30% spent 6-10 hours a week researching, and a further 22% spent more than 10 hours a week keeping up with the latest trends and methods.

There's no reason to doubt that malicious attackers are even more well-informed and motivated to stay ahead of the defenses that organizations will throw their way. Considering almost half of our respondents claim they can breach security in less than six hours and an equal number say they can exfiltrate data in a similar timeframe, how much damage can a malicious attacker do in a week? Or a month?

A large number of respondents—close to 30%—advised "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."

The question is, how can we build actionable intelligence about our threat landscape and properly protect our data?

We need a holistic solution. We need education and robust security policies that cover everything from governance to response and remediation. We need endpoint solutions that can protect against sophisticated malware and ransomware outbreaks—and even provide some sort of mitigation for social engineering attacks.

What's very much lacking is a solution that ties everything together and allows you the flexibility to respond to all of the threats your organization faces. The majority of our respondents say they change attack tactics regularly or even with every engagement; why would you want to combat that with a rigid, outdated approach to security? You'll never come out on top.

We need to understand that security is more than just a policy on a piece of paper, an antivirus program, or a group of professionals sitting in a room scanning log events. It's all of the above, and it's piecing everything together in a way that makes sense.

That's the true challenge that we face in our industry today and it's one I'm confident we can overcome.

Stuart Clarke – Chief Technology Officer, Cybersecurity, Nuix

Stuart is an internationally respected information security expert who is responsible for the overall security and intelligence strategy and delivery at Nuix. He has advised the United Nations' peak cybersecurity body ITU and provided cybersecurity training for over 60 national computer emergency response teams.


SECURITY
COUNTERMEASURES

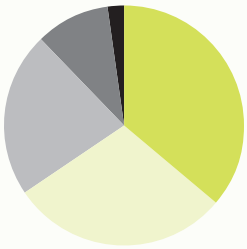
One of the most compelling aspects of our research were the findings regarding the effectiveness of security countermeasures. These findings will help security decision makers understand which aspects of their defensive posture really work and which are little more than items on a checklist. If your defenses do not line up with the experience of those who are attacking you, there is a serious flaw in your defensive posture and your organization's critical data is in considerable danger.

The number one most effective countermeasure, according to 36% of respondents, was endpoint security. This was followed by intrusion detection and prevention systems at 29% and firewalls at 10%. Only 2% of respondents were troubled by antivirus. Interestingly, 22% of professional hackers boasted that no security countermeasures could stop them and that a full compromise was only a matter of time.

For security decision-makers, this result clearly demonstrates the importance of defense in depth rather than relying on any single control. Any individual security control can be defeated by an attacker with enough time and motivation. However, when an organization uses a combination of controls along with security training, education, and processes, the failure of any single control does not automatically lead to data compromise.

In addition, if technological controls can all be bypassed, end-user education is among the most critical components of any organization's security posture.

Which security countermeasure presents the greatest challenge to you during a penetration test?



- Endpoint security 36%
- Intrusion detection/prevention systems 29%
- Nothing can stop me—it's just a matter of time 22%
- Firewalls 10%
- Antivirus 2%

Based on their experience breaking into corporate systems, professional pentesters offer a unique and valuable perspective on where security decision makers can spend their money most effectively. More than a third of respondents (37%) believed intrusion detection and prevention systems represented the best return on investment while another quarter would, perhaps not surprisingly, put their money into goal-oriented penetration testing. Twenty-one percent felt that data hygiene and information governance represented the best investment—an interesting result, as we will soon see.

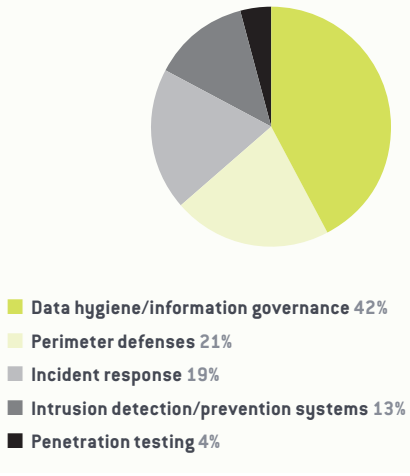
Where do you think is the most effective place to spend security budget?

- Intrusion detection/prevention systems 37%
- Penetration testing 25%
- Data hygiene/information governance 21%
- Incident response 10%
- Perimeter defenses 6%

On the flip side of the previous question, we asked pentesters what they thought was the least effective measure on which to spend security budget and 42% nominated data hygiene and information governance. Clearly information governance elicits strong opinions from professional hackers. On the one hand, if organizations achieved the goal of information governance, they would have all their data goodies in one area, ripe for compromise. On the other, information governance used in conjunction with other security controls can provide another layer of defense in the protective web I discussed earlier.

Equal second, or near enough, were perimeter defenses (21%) and incident response (19%) as ineffective ways to spend security dollars. We're curious about the 4% of professional pentesters who thought that goal-oriented penetration testing was the least effective place to spend security dollars.

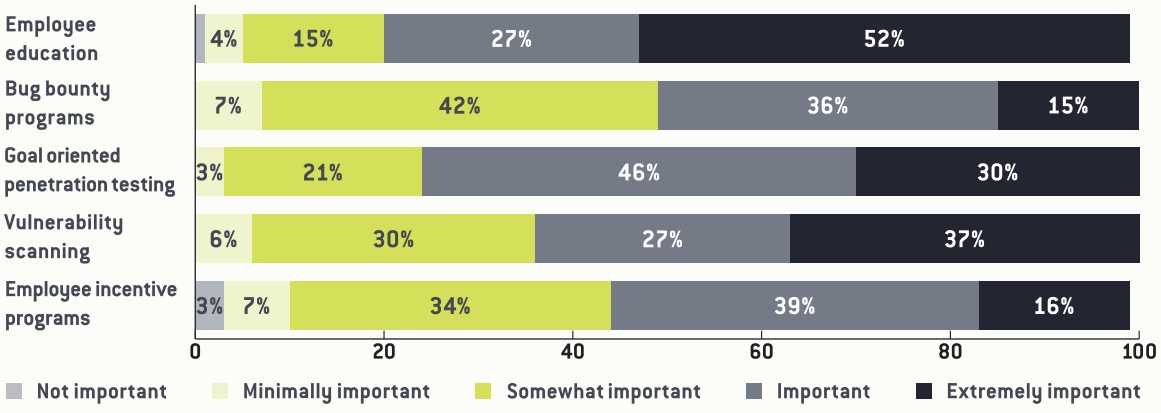
Where do you think is the least effective place to spend security budget?



For a nuanced look at the most and least effective security practices, we asked respondents to rate five security countermeasures from not important to extremely important in their ability to prevent attacks.

More than half (52%) said employee education was an extremely important countermeasure and 37% were strongly in favor of vulnerability scanning. A large proportion of respondents (42%) only rated bounty programs as somewhat important.

Rate the importance of the following security countermeasures in preventing cyberattacks



RANSOMWARE AS A SERVICE

Ransomware is projected to be a billion-dollar-a-year industry.[1] It's almost certain you or someone you know will be a victim. The emerging marketplace for ransomware provides some fascinating insights into how easy it is for would-be cybercriminals to get started.

Like any good entrepreneurs, the authors of ransomware have not just profited from running their own operations, they've also begun selling their services for a cut of the action. This business model is commonly referred to "ransomware as a service" (RaaS). One of the first RaaS kits was called Tox.

Tox allowed users to create a custom ransomware sample by visiting a specific Tor site. Once on the site, the user would enter in the ransom note, ransom price, and a verification code. After that, the Tox service would generate a 2 MB executable file disguised as a screensaver that contained the ransomware code.

Shortly after Tox debuted in 2015, other RaaS kits followed including Fakben, Encryptor, and Raddamant. As they grow in popularity, the prices for ransomware kits are being driven even lower.

A recent search of malware forums revealed RaaS kits for sale ranging in price from $15 to $95.

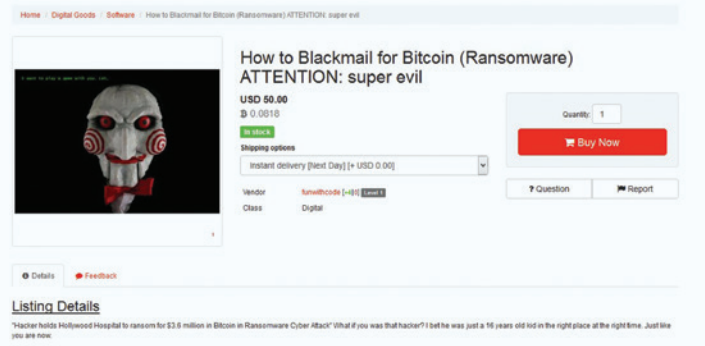
Figure 1: Ransomware kit for sale on a private online marketplace.

Figure 2: Ransomware kit for sale on a private online marketplace.

[1] David Fitzpatrick and Drew Griffin, Cyber-extortion losses skyrocket, says FBI, *CNN*, April 15, 2016

[2] Michael Kan, Cerber ransomware rakes in cash by recruiting unskilled hackers, *CSO*, August 16, 2016

Figure 3: Ransomware kit for sale on a private online marketplace.



A Variety of Business Models

In fact, there are a number of business models available for a would-be ransomware criminal. Underground forums are actively selling variants including:

- Shark, with no upfront cost but the developer takes a 20% cut of the ransom
- Cerber, which generated its authors over $75,000 just in July 2016
- Stampado, which sells for $39 and grants the buyer lifetime access to the kit.

Cerber is believed to originate in Russia and has been posted on underground forums by a user named 'crbr'. It's estimated that nearly 150,000 machines were infected with Cerber in July and that the yearly profit for Cerber will top one million dollars.[2]

Since 2014, the number of victims of ransomware has grown by 550% and nearly half of these will pay the ransom. With the ease of use that RaaS kits offer and the billion-dollar industry that the ransomware authors have created, it's easy to see why this attack method is spreading so rapidly.

Exploit Kits

Any discussion of ransomware should include an overview of exploit kits, a common delivery method. Believe it or not, it is getting harder to simply email an executable attachment to a victim and convince them to open it. Exploit kits are shortcuts that make it easier to deliver malware and get it to run on a victim's machine.

The first known exploit kits, WebAttacker and Mpack, were released in 2006. In the 10 years since, the exploit kit market has expanded, becoming more sophisticated and dangerous.

Traffic is typically driven to an exploit kit in three ways (see Figure 4):

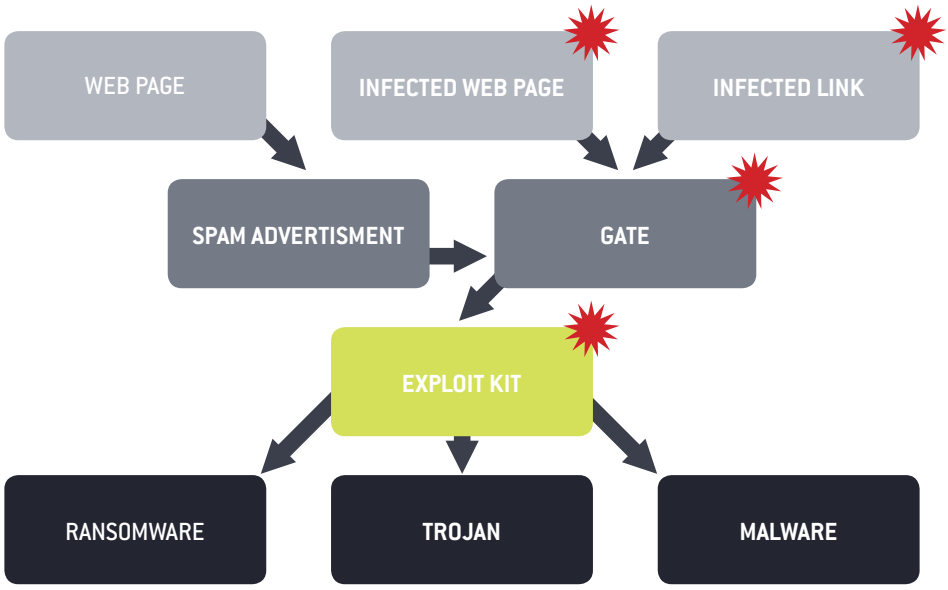
- **Phishing.** Email scanners have much improved their ability to scan for malware and potential malware traveling through their system, which means emailing a malware executable to someone is largely not an available option anymore. However, crafty attackers can send spam messages to users enticing them to click on hyperlinks. These links can point to an exploit kit (or the gateway to an exploit kit). If the user's browser or operating system isn't protected well enough, the ransomware is delivered.
- **Compromised websites.** Once a website has been compromised, the bad actor can introduce code that sends the web browser to the landing page of an exploit kit or a gateway to an exploit kit—often using a hidden ‹iframe› or inline frame tag. The traffic redirector or gateway system determines that this is traffic it would like to pass to the exploit kit. The exploit kit then probes the system for vulnerabilities and, if one is available, delivers the ransomware payload.
- **Malvertising.** Malvertising works similarly to the compromised website method listed above except the redirection code is contained within paid advertising on a usually highly trafficked website. The user doesn't even need to click on the advertisement to have their traffic redirected to the exploit kit.

Exploit kits are now also available as a service. Using a subscription model, the authors of exploit kits have simplified the attack

and made it much more efficient and effective. A bad actor now simply needs to divert traffic toward the exploit kit to which they subscribe—and the kit is continually updated with new exploits.

Stopping these exploit kits is like trying to kill a hydra. As exploit kits are taken down or their creators are arrested, criminals seamlessly shift to one or two other emerging kits providing similar services. For example, following the demise on the Angler toolkit in mid-2016, customers quickly shifted to the neutrino and RIG exploit kits. As of October 2016, RIG was the most popular exploit kit on the block.

Figure 4: Methods of driving traffic to an exploit kit.



Chris Brewer – Cybersecurity Consultant, 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 security analyst.

Andrew Spangler — Principal Cybersecurity Consultant, Malware Analysis, Nuix

Andrew is a security researcher with over 20 years' experience. He works with Nuix's incident response, forensics, and penetration testing teams to provide reverse engineering, tool development, and malware analysis services. He has written technical analyses on cutting-edge malware families.

ON ORGANIZATIONAL INCIDENT READINESS

Information security, incident readiness, and data breach response are being discussed in nearly every executive and board meeting, in just about every business around the world. Every day we learn of new breaches, new regulations, new security frameworks, and new litigation in the wake of some large data theft or loss.

Organizations are now spending more of their precious time, resources, and budgets obtaining and implementing data breach prevention and monitoring technologies such as system endpoints and network assessment appliances. They train their organizational leaders and technologists, put incident response plans into writing, and still suffer breaches. What is going wrong?

A False Sense of Security

In my experience—I've been working as an incident responder and security architect for more than a decade—organizations that start to prepare seem to suffer from a false sense of security. They set the pieces in motion but they never actually "play the game."

For example, an organization may do a mock exercise and walk through an incident response plan but very few take the time to sit down and have real-world (controlled) attacks performed against them while the response and monitoring teams are watching, reacting and learning, in near real time.

Even worse, many times when security teams detect an anomaly, they immediately take the affected systems offline and replace them with a fresh image. This destroys critical evidence and the ability to learn from it. This evidence may be required later on for the purpose of assessing organizational damage or as part of legal or HR actions. Wiping the breached system means you can never conduct root cause analysis or exercise a corrective action or remediation plan. So great job! You remediated this incident. But you also failed to prepare yourself to deal more effectively with the next one.

Visibility Starts with Data Sources

Very few security teams can make the leap from looking at alerts on a screen to actually detecting and mitigating threats. They don't know what they are looking at or looking for. What forensic traces does a real attack leave behind when an attacker dumps credentials? When they are actively looking for new targets? When they are downloading your databases? What are the precursors to an attack? How is this activity different from day-to-day business on your network that your IT pros can safely ignore? What are the business needs for that treasure trove of data? Sadly, the majority of organizations simply can't answer these questions.

Combatting this lack of visibility starting with taking an inventory of your data sources. What data sources are available within your organization? Where are your data gaps? Which data sources can answer (confirm or deny) questions about a security event within your environment?

Get Comfortable with Logs

Logs are often invaluable during an investigation. A successful logging program begins with creating, standardizing, and retaining logs. Many organizations still rely on inadequate default settings for logging instead of customizing those settings based on their specific organizational threat model. Is your most critical data in a web server or in your human resources system?

Internet–facing systems such as web servers are commonly under-configured for logging or retention; many network services such as DNS and DHCP aren't logged at all. However, these logs can be highly valuable during an investigation, so you should retain them in a central repository rather than on the servers themselves. The key is understanding where the data you need is located and preserving it where it cannot be tampered with, altered, or deleted.

Specific to Microsoft Windows systems, make sure granular logging is enabled (especially for PowerShell) and keep the logs in a central repository rather than overwriting them as soon as the buffer size is met.

Review these logs frequently and understand what constitutes normal versus abnormal behavior. Automate and incorporate alert logic that makes sense for your environment; iterate and modify as necessary—this is an ongoing process that requires constant attention and effort.

Take Forensic Images Before You Nuke Systems

Retaining logs is especially important if your organization practices "nuke from orbit" recovery tactics. Investigators understand that wiping and reimaging affected systems is the fastest road to get a user or server back up and functional but it is a terrible practice. When you wipe that hard drive, you have no idea what the impact may be a month later, let alone six, or nine months later.

The average time it takes an organization to discover a breach is anywhere from 250–300 days, depending on which threat report you're reading. When a third party, such as an incident response specialist or a law enforcement officer shows up, can your organization identify the system owner, the location, and the physical box based on an internet protocol (IP) address on a specific date? Can you guarantee that system you just wiped out was not part of something larger, perhaps criminal activity? Is this anomalous behavior or something more nefarious? If you don't know what led to the breach, can you prevent it next time?

Preserving data is no longer a serious challenge. High-capacity hard drives and long-term storage are very inexpensive. The tools required to preserve forensic images are free or very low in price.

Consider your retention policies. How long do you hold your log or source data? Do you have a regulatory requirement for retention? How far back can you evaluate an event within your organization?

Become the Organization You Need to Be

How do we move forward and become the organizations we need to be?

- Build an incident response plan and then test it, fix it, and test it again.
- Never stop asking yourselves, what's next?
- Iterate, Iterate, Iterate.
- Determine whether you have the people, technology, and processes to detect breaches and to defend against them.
- Once you make the determination, go to work! Find and fill the gaps in your armor to give your responders a fighting chance of responding in a timely manner.
- Break away from the normal security mindset; learn where other organizations have failed and don't fall into the trap of "feeling" secure.
- Plan. Test. Retest.
- Attack. Learn. Fortify.

Like a good battlefield commander, know where your line is strong, know where your line is weak. Know your battlespace, think like your enemy. Don't wonder if you are secure—know.

Grayson Lenik — Principal Security Consultant, Digital Forensics & Incident Response, Nuix

Grayson has worked in information security and digital technology for more than 20 years. He regularly instructs law enforcement and private industry in hacking techniques, incident response, and digital forensics and has researched and presented on anti-forensics, cybercrime operations, and incident response methodology.

FRUSTRATIONS AND FOLLOW-UP

Every job has its frustrations but when a professional pentester is frustrated it's probably a good indication that something is not right in your cybersecurity defenses. The biggest frustration for nearly two-thirds (64%) of the professional penetration testers and hackers we spoke to was that organizations didn't fix the things they knew were broken. This is a very significant finding, since no one within your organization will know and understand your security weaknesses more so than the folks that are hacking you.

For the remainder, 10% were frustrated by what they saw as a fundamental lack of understanding of cybersecurity and 10% gave other reasons such as improper or basic IT hygiene, missing patches, and a general misunderstanding of security by decision makers. Worryingly, 8% felt like they were misunderstood and victimized when all they wanted to do was make things better.

What is your biggest frustration as an attacker?

- People don't fix the things that they know are broken 64%
- Corporations and governments just don't "get it"—I want to get paid just like them; no one's getting hurt by what I do 10%
- Other 10%
- Security technologies make it difficult to get what I want to get 8%
- I am victimized for what I do, when all I want to do is make things better 8%

What Comes After a Penetration Test?

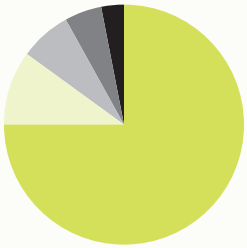
After an organization engages in a penetration test, in the experience of three-quarters of respondents, it only conducts limited remediation, usually focused on critical and high vulnerabilities. Only 10% of respondents indicated that they saw full remediation of all identified vulnerabilities, and subsequent retesting.

While "fix the biggest problems" appears to be a logical approach to remediation, it misrepresents the true nature of vulnerabilities and provides a false sense of security for decision makers. If you only address specific vulnerabilities that you have chosen arbitrarily and devoid of context, it's the cybersecurity equivalent of taking an aspirin for a brain tumor; you are addressing a symptom as opposed to the root cause.

Simple remediation of specific vulnerabilities fails to take into account why that deficiency exists in the first place; it discounts strategic shortcomings such as poor or missing patch management policies, lack of a vulnerability management program, or untrained security staff. This approach also fails to recognize the complexities of multi-staged attack vectors. For example, while certain security flaws may have low or medium Common Vulnerabilities and Exposures scores (a ratings systems maintained by the United States Department of Homeland Security), these same vulnerabilities combined with others can give the attacker access to the target or the ability to escalate privileges. A third problem with focusing on vulnerability remediation is that many leveraged escalation points are security misconfigurations, not vulnerabilities in the classic sense.

A big worry is the 5% of respondents who said they saw no remediation whatsoever after they conducted tests.

After an engagement, what is the organization's most common action?



- Some remediation; usually focused on high and critical vulnerabilities 75%
- Full remediation; all vulnerabilities are remediated and re-tested 10%
- Extensive remediation; most of the identified vulnerabilities are remediated, regardless of ranking 7%
- Nothing; they were just checking boxes 5%
- Other 3%

RESILIENCE: THE MISSING PIECE OF A SECURITY PROGRAM

How resilient is your organization when it comes to cyberattacks? How can you become more resilient?

In general, resilience is the ability to return to health or success after something bad happens. From a security perspective, resilience is the ability to remain operable during a security event and to recover afterwards in a timely manner.

This is important because the majority of professional hackers we surveyed (88%) said they could compromise systems in less than 12 hours and a similar number (81%) said they could exfiltrate data in the same timeframe. Half of respondents change their attack methodologies every time they're engaged to compromise a target.

In other words, you can pretty much guarantee your organization will suffer some sort of successful cyberattack against it no matter how well you keep your preventative controls updated.

But Hacking Is Illegal...!

What can you do if your preventative controls aren't enough? Some people outside the security profession think the fear of legal repercussions will persuade hackers to leave their systems alone. This is utterly unrealistic. More than 80% of the hackers we surveyed said they got caught in the act less than half the time. Even if the breached organization has appropriate detective measures, skilled attackers are very adept at covering their tracks.

Attribution—identifying precisely who is responsible for an attack—is tremendously difficult for forensic investigators and law enforcement. Even with successful attribution, unless your attackers are based in the same country as you, you'll need to get them extradited under a mutual legal assistance treaty. This takes around 10 months—longer in some cases—giving the attacker plenty of time to find out about the request and temporarily relocate to a non-extradition country.

Essentially, cybercriminals can act with impunity and if you have something worth stealing, they'll try to steal it.

Surviving a Breach

If you can't prevent a breach, you must be prepared to survive it. What does this resiliency look like? It's about understanding your organization's risk tolerance and finding an appropriate balance between the three elements of the security triad: confidentiality, integrity, and availability.

Confidentiality

Confidentiality means that only authorized users can access systems or data. This is usually done through access control lists at the network, system, or application level and by hiding data using encryption or tokenization.

A resilient system will provide easy ways of revoking users' access; changing the encryption keys or tokenized values; and updating the data sets that were compromised. For example, if an organization discovered that a password store has been compromised, it would need to enforce password updates, lock some users out, identify if individual user IDs have been compromised, and monitor access to those users' data.

Integrity

Integrity refers to the trustworthiness of data, ensuring it has not changed during transit or copying, or been modified by unauthorized people or processes. Disk monitoring tools can verify the integrity of applications but are much less effective with data directories that are constantly changing. Data integrity can be handled using hashes and hash message authentication codes (HMACs).

A resilient system is one where you can restore lost data, regenerate hash values or HMACs, and redeploy the appropriate configuration of systems and networks from a known good install. External monitoring mechanisms can also help you identify integrity gaps.

Availability

Availability is the ability of authorized people to access the system when they need to. Keep in mind, a system may not need 99.999999% uptime; it may only need to be operational during business hours, for example.

Achieving a Balance

How an organization balances these three elements depends on its priorities. For a bank, integrity of data is paramount, while a healthcare organization needs to maintain confidentiality as well as integrity. An online retailer will probably prioritize availability.

Testing your organization's resilience should be part of your disaster recovery and incident response plans. You need to test these scenarios regularly to build up your organization's resilience to security events.

Systems that contain valuable information are bound to be breached at some point. How resilient your organization is to these breaches will ultimately determine how long the organization remains in business.

[1] Yury Izrailevsky and Ariel Tseitlin, The Netflix Simian Army, *Netflix Tech Blog*, July 19, 2011

Evan Oslick — Software Security Developer, Nuix

Evan works as a security professional focused on helping developers build secure software. He has worked in the application security space since 2004 after spending 10 years as a software engineer.

A POLICE CHIEF'S EVOLVING PERSPECTIVE ON CYBERSECURITY

Nearly everything in the criminal investigative world is now touched by an element of cybersecurity. Evidence that used to be kept in personal address books, drawers, filing cabinets, and handwritten mail now comes in digital form. Criminals communicate via cell phone, text messages, social media, and even video games. Just as police agencies were getting used to video from crimes scenes being posted on the internet after the event, criminal acts are now being broadcast live to an online audience.

Cybertheft and Cyberattack

Not too long ago, all police departments needed to worry about was making their buildings physically secure and their computer systems password protected. Now cyberattacks on police systems and cybertheft of data contained within police computer systems are commonplace. Sensitive information such as personnel files, informant testimony, and investigative case data are routinely hacked. An officer-involved shooting that draws national attention immediately makes your agency the target for hackers.

When a police agency comes under cyberattack, it is often in the form of ransomware. Cybercriminals hack into police databases and encrypt them so that they are unusable. The only way to get access back to the invaluable data is to pay a ransom.

Encryption "Going Dark"

Police also face the issue of "going dark."[1] Encryption on modern smartphones and PCs is so sophisticated that law enforcement can't access digital criminal evidence even with a court order. This allows criminals to communicate with impunity and conduct organized crime business without fear of police access, even when lives are at stake. This should seriously concern every law-abiding citizen. Unfortunately, it is likely to take a catastrophic incident or a series of catastrophic incidents to wake up those who are most vulnerable and to draw the attention of our police executives.

In 2013, the International Association of Chiefs of Police and the Canadian Association of Chiefs of Police conducted a survey of police executives finding that 79% of respondents rated the risk of a cyberattack as moderate to very serious.[2] However, only 13% of police executives surveyed said they regularly engaged a third party to audit their systems and only 33% had ever had a cybersecurity audit. This appears to be an issue of priority more than one of awareness. The survey also found that respondents only took cybersecurity threats more seriously after they had been attacked.

Improved Forensic Examination Practices

In addition, the scientific community is strongly recommending reform of current police forensic examination practices. The concerns are based on scientific principles and sound reasoning.

Specifically, the scientific community recommends scientifically validated forensic quality assurance improvements. In some areas, police forces must gain American Society of Crime Laboratory Directors (ASCLD) accreditation for evidence processing and analysis in order to be properly validated for use at all levels of the criminal justice system. This will become a high priority for law enforcement executives in the very near future—affecting budgets, operational capacities and even the ability to successfully prosecute criminal cases.

The National Institute of Justice has been working with professional police organizations for many years to improve forensic analysis toward scientifically proven standards. In 2009 the National Research Council released a report very critical of current forensic analysis practices in the United States.[3] The President's Task Force on 21st Century Policing Final Report recommended

[1] James Comey, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, address to Brookings Institution Washington, D.C., October 16, 2014

[2] International Associations of Chiefs of Police and Canadian Association of Chiefs of Police, Law Enforcement Perceptions of Cyber Security, proceedings of 2013 LEIM Conference Workshop, May 22, 2013

"The US Department of Justice, in consultation with the law enforcement field, should broaden the efforts of the National Institute of Justice to establish national standards for research and development of new technology."[4]

More recently the LA Times reported the President's Council of Advisors on Science and Technology would soon issue a report critical of subjective testimony by experts linking evidence collected to specific people, objects, locations, and events. Though the report is focused more on non-digital evidence, it calls into question analysis that links firearms to shell casings, indicating that this analysis "falls short" of scientific standards for admission as evidence.[5]

Cybersecurity investigators and analysts and police executives should all heed today's professional scientific narrative. Law enforcement methods, procedures, policies, and practices must begin to align with scientific standards and recommendations. Professional law enforcement organizations, private cybersecurity organizations, and law enforcement agencies must embrace recommendations that reduce the potential for error.

Data Storage and Security

While the impact of digital evidence on law enforcement continues to evolve, what will remain consistent is the need to identify, collect, analyze, disseminate, store, and secure such evidence. The areas that are currently evolving most rapidly are analysis to a scientific level along with related evidence storage and its security. One specific development in recent years is driving vast numbers of US law enforcement agencies toward cloud storage.

The national dialog that emerged since the shooting of Michael Brown in Ferguson, Missouri has resulted in a call for independent review of police use of force. Community and law enforcement leaders have turned to body worn cameras (BWCs) to document police actions. Placing BWCs on every police office in any police agency creates vast amounts of digital video evidence. To store these large volumes of data, many law enforcement agencies have contracted with private vendors for cloud storage services.

Collection and storage of digital evidence is concurrently growing in many other areas of criminal investigation including crime scene photography, identity theft, and accident reconstruction. The growth in digital evidence increases the risk of a cybersecurity breach. This also increases the potential harm to an agency because a breach could negatively impact pending criminal or civil cases. A breach of a popular cloud store vendor might affect many agencies simultaneously.

Educate Yourselves

The impact of cybersecurity on law enforcement and the criminal justice system is just beginning to define itself. Digital evidence and forensics are a growing part of criminal cases. Analysis and storage of digital evidence requires collaboration between the public and private sectors to ensure we apply appropriate scientifically approved analysis and use validated secure storage systems. It is imperative for law enforcement executives to educate themselves in cybersecurity measures to ensure their data is protected and independently audited against intrusion or tampering.

[3] National Research Council of the Academies, *Strengthening Forensic Science in the United States: A Path Forward*, August 2009

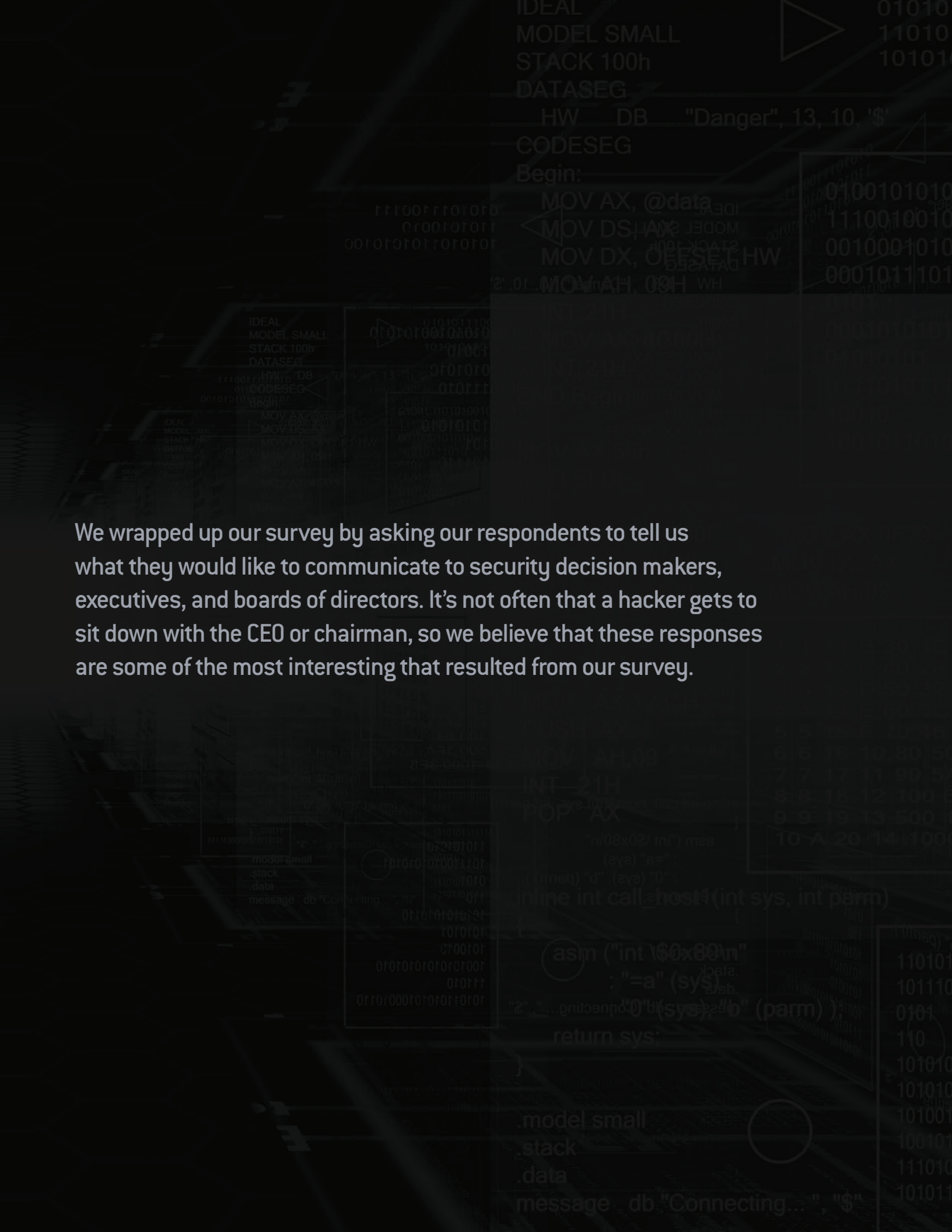
[4] Office of Community Oriented Policing Services, *Final Report of the President's Task Force on 21st Century Policing*, May 2015

[5] Del Quentin Wilber, White House panel expected to issue report critical of some forensic evidence in criminal cases, *Los Angeles Times*, September 1, 2016

Terry L. Sult—Chief of Police, Hampton, Virginia

Terry began his law enforcement career at age 14 as a Police Explorer and Civilian Police Dispatcher and became a sworn officer in 1978. He was Chief of Police in Gastonia, North Carolina; Police Chief and Director of Public Safety in Sandy Springs, Georgia; and has been Police Chief of Hampton, Virginia since 2013.


MESSAGE TO
EXECUTIVES



We wrapped up our survey by asking our respondents to tell us what they would like to communicate to security decision makers, executives, and boards of directors. It's not often that a hacker gets to sit down with the CEO or chairman, so we believe that these responses are some of the most interesting that resulted from our survey.

The largest proportion of respondents (44%) believed security was important to boards of directors and that they viewed it as essential to the future success of the business. However, another 30% had a more cynical view that boards were only interested in security for compliance reasons and 15% said they were only doing the bare minimum.

How do you think your board of directors perceives security?

- Security is important to us, and to the future success of our business 44%
- We have to deal with security for compliance reasons, nothing more 30%
- Companies get hacked every day—it's the new normal; we should do just enough to show we think it's important but no more 15%
- Other 7%
- Security is a waste of time and money; I don't need or want to know about it 5%

Given the opportunity to speak to security decisions makers, the penetration testers we surveyed would say:

- "You will never be secure. This is journey, not a destination. Get used to the idea that security is not a part of normal business operations." **(30%)**
- "Training your staff is going to have the biggest impact on your overall security. You need to turn your weakest link into your greatest asset." **(26%)**
- "You need to have a strong marriage of people and technology. If the problem were able to be solved by one or the other, it would have been solved years ago." **(20%)**
- "Assume humans will fail to be secure; you need to look at technical security controls that will protect people from themselves." **(13%)**

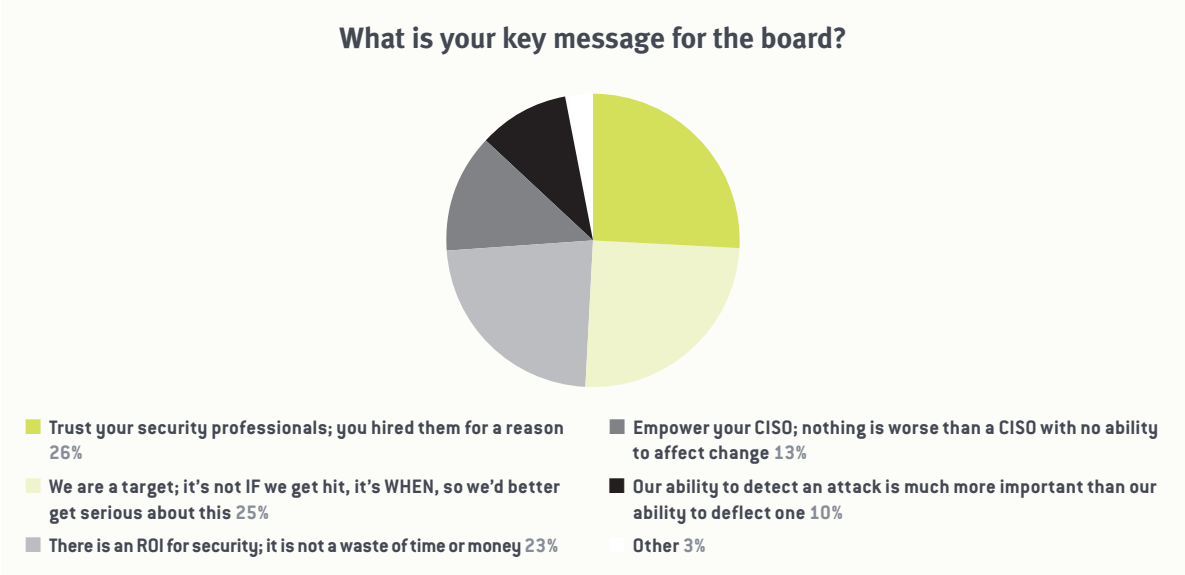
What is your key message for security decision makers?

- You will never be secure; this is a journey, not a destination 30%
- Training your staff will have the biggest impact on your overall security 26%
- You need a strong marriage of people and technology 20%
- Assume humans will fail; look at technical security controls that will protect people from themselves 13%
- Other 11%

Our final survey question asked pentesters what they would like boards of directors to hear. They said:

- *"You need to trust your security professionals. You hired them for a reason ... let them do their jobs!"* **(26%)**
- *"We are a target, without question and without exception. It's not IF we get attacked, it's when. So, we'd best get serious about security!"* **(25%)**
- *"There is a return on investment for security; it's not a waste of time or money."* **(23%)**
- *"You need to empower your CISO! Nothing is worse than a CISO with no ability to effect change!"* **(13%)**
- *"Our ability to detect an attack is more important than our ability to deflect one."* **(10%)**

It seems the overall conclusion is about cyber-resiliency. If it's a forgone conclusion that an attack is imminent, organizations need to expediently and precisely figure out if an attack has indeed taken place, quickly understand the breadth and depth of the attack, and then formulate a response strategy. In this situation, the Board needs to trust that the organization's security professionals understand the threat landscape and are willing to work with the other groups (IT, developers, legal, HR, etc) to limit the amount of downtime or exposure to a breach.



NAVIGATING THE LEGAL MINEFIELD OF POST-BREACH RESPONSE

Every year, dozens of class actions are filed against companies that were the victims of data breaches. The breaches at issue run the gamut of causes—accidental loss of an unencrypted thumb drive containing patient data; spear-phishing emails that ended with an employee emailing details of the incomes of the company's employees to hackers; and point-of-sale systems infected with malware resulting in the compromise of payment card information.

From the allegations in these lawsuits, it appears the public believes these companies did not care about cybersecurity, deliberately implemented insufficient information security policies (or none at all), and upon discovering the breach, did nothing but count their money and strategize how to do the least possible in response.

Nothing could be further from the truth.

What Really Happens After a Breach

In the immediate aftermath of a breach, companies are scrambling—assembling their incident response teams, engaging legal experts to ensure compliance with laws, engaging forensics firms to assist with the investigation, determining what happened, and ensuring the system has been restored and cleaned. They're writing and rewriting the communications to their customers or clients, employees, and members to ensure they receive accurate information in the very short time frame permitted by many breach disclosure laws. They're also reviewing the ever-changing regulations in all the jurisdictions they operate to ensure all communications are legally compliant. And they're weighing the decision whether they should provide credit monitoring or identity restoration services to the impacted population—which some courts might view as proof that the company knew the impacted population was at risk of identity theft.

Complicating the issue, some statutes provide that the compromise of a credit or debit card number without a security code does not require notification. So even if a card holder's name, address, and full credit card number was compromised, companies would only be required to notify individuals in a handful of states in the US and some other countries. Even so, many companies voluntarily notify individuals and state regulators of a breach because they're concerned about the harm to the company's reputation if customers learned of the compromise through another means. This notification, in turn, can increase the level of visibility of a security incident and thus the possibility of litigation.

Credit Card Fraud Is Not Identity Theft ...

The allegations plaintiffs make in data breach cases are frequently ridiculous. Plaintiffs often conflate credit card theft and financial fraud with wholesale identity theft. The former has fairly isolated consequences—fraudulent charges that are uniformly reversed by the credit card company—the latter has

long-term effects on individuals' credit scores and applications for credit.

Plaintiffs allege that because they had their credit card numbers stolen, they were required to monitor their credit reports and purchase credit monitoring products. But these products monitor a consumer's general credit file, not the individual credit cards and their transactions. Plaintiffs also argue that breached organizations must supply credit monitoring products because, now that their credit cards have been stolen, they are at an increased risk of identity theft. But that ignores the fact that you simply cannot steal a person's identity with just their credit card number. These specific and extremely flawed allegations are critical for these class actions to continue—without these "damages" there would be no case.

Unfortunately, courts have allowed themselves to get tangled up in these allegations. Just this year, courts found support for the conflation of credit card theft and identity theft in two places: the decision to provide credit monitoring and the inclusion of statutorily required language in notification materials. These decisions, elevated beyond mere business decisions and compliance, have become deciding factors in whether a breached company will face a long and costly legal battle.

… But the Courts Think It Is

For example, in *Remijas v. Neiman Marcus Group, LLC*, 794 F. 3d 688 (7th Cir. 2015), the court stated that "[i]t is telling . . . that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores" during the time malware was active on the store's computer system.

From this offer, the court determined that there must be a risk of identity theft because why else would Neiman Marcus offer credit monitoring? The actual answer to that question might be because it is a token of goodwill to customers who feel vulnerable, or because people expect it these days, or because it may mitigate the anger, and thus the desire to sue, that affected individuals feel.

In *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F. 3d 963 (7th Cir. 2015), the court stated that by including in its press release that consumers should monitor their credit reports "rather than simply the [credit card] statements for existing affected cards," P.F. Chang's "implicitly acknowledged" that the card data stolen by hackers could be used to open new cards in the consumer's name. This despite the fact that data breach notification laws in many US states—including Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Virginia, Vermont, and West Virginia—require entities to use that kind of language when they notify their customers.

The court in *Remijas* also accepted that the information stolen from payment cards could be used to open new cards in the consumer's name. That position is highly doubtful, as anyone who has opened a credit card knows they must provide

much more proof of identity than a credit card number to be approved for a credit card. And in many cases, the name of the cardholder has not been compromised, much less the billing address, Social Security number, or mother's maiden name.

Why the System Is Stacked Against Breached Organizations

This problem arises, at least in part, because of the way lawyers are constrained when moving to dismiss a case. During the early stages of a lawsuit, lawyers cannot argue common sense or plead with the judge to reach into his or her personal experiences. They cannot offer the court outside experts to explain how identity theft occurs and why credit card theft is different; how skimmers work; or what data is embedded on magnetic stripes on credit cards and, more importantly, what is not.

Procedurally, the first time the defense has an opportunity to educate the judiciary is a year or more into the case, after the parties have already paid hundreds of thousands of dollars in legal fees and discovery expenses. Companies cannot stomach the thought of getting that far, paying that much, and still having the judge find against them. And so they settle.

Until there is an opportunity to educate the judiciary on what constitutes identity theft or a legitimate risk of identity theft, companies must tread carefully when responding to a data breach. Failure to do so means the organization may end up facing a court that allows a case to proceed because of public statements made in response to a data breach, or one that thinks an offer of credit monitoring is evidence that a person's identity is at risk.

Melissa K. Ventrone – Partner, Thompson Coburn LLP

When a cybersecurity incident strikes, Melissa and her team work around the clock to control a breach situation and manage any public or regulatory fallout. She also represents her clients in cybersecurity litigation and the proactive management of data privacy and security risks.

Aleksandra M. S. Vold—Associate, Thompson Coburn LLP

Aleksandra helps clients prepare for, safeguard against, and aggressively respond to cybersecurity breaches. Her practice includes privacy breach response, payment card industry standards and investigations, advising on data privacy and security risk management, and class action privacy litigation.

YOUR BIGGEST CYBERSECURITY THREAT: FAILING TO PLAN

It's surprising how often the simplest phrases can provide the most salient advice. The 6 P's, for example: Proper prior planning prevents poor performance. While the phrase may be a bit of a tortured alliteration, the truth and simplicity of its sentiment can't be denied: When you want a good outcome, you have to think it through. Simple. Straightforward. To the point.

So why are so many boards and C-suites screaming into the void about how to handle cybersecurity? The answer couldn't be clearer—they just need to plan it.

Now, simply directing a board or executive to "plan cybersecurity" sounds pedantic. But it really is that straightforward and it really does need to be done from that level.

An Executable Plan for Executives

The good news is that since we are starting in the executive ranks, the plan being developed simply needs to be executable. It does not need the level upon level of details that the execution will eventually bring. Rather, it needs to be executed at a high level and give management the questions and guidelines they will need to put into effect what will become a comprehensive and holistic approach towards cybersecurity.

So, with that in mind, sit down with a pencil and a piece of paper and get started. There is no need to find gadgets and gizmos. No need to track down network and IT expertise. Rather, it starts with one simple question, written on the top of the page:

How do we **secure** our **data**?

Simple thesis, right? But note the three bold words. Each is critical to where this thesis will lead your planning.

How

"How" is really a two-fold question: how are you doing it now and how should you do it in the future.

The first part of the question is a candid self-assessment of where the organization is right now. For many organizations, this is a journey into a world you do not want to wander. Unfortunately, want doesn't have a place in the equation, it's a no-kidding need. Organizations need to honestly assess what they are doing to secure their data.

This raises the first and perhaps most important sub-question: Who should perform this assessment? To start, you need to know who is in charge of the organization's cybersecurity right now. Is it IT? Legal? Compliance? Janice in accounting? Whoever is responsible for cybersecurity needs to be on the hook to tell management how well they think they're doing. That report must be as inclusive as the assessor can make it and, to be honest, it is very much a test that will be reviewed and graded by management.

Fortunately, management can outsource the task of grading that report—and I strongly recommend you do this. This means hiring a third party (preferably under the auspices of counsel) to come in and perform an assessment of the assessor.

This is such an important step.

No offense to your IT team members (or Janice from accounting), but why ask the fence builder how secure your fence is and take them for their word? That's not how it's done. There are far too many variables that someone on the inside might miss.

Use a vendor, under attorney-client privilege, to better understand how prepared the organization—and its key staff—is to secure the organization's data. And when you identify issues, endeavor to fix them in order to stay secure.

Secure

Surprisingly, "secure" is a concept often overlooked in cybersecurity planning. Generally, organizations focus on legalistic terms such as "compliance" and "reasonable" and lose sight of the ultimate goal, which is security. They forget that by aiming for security, they can achieve compliance and reasonableness along the way.

Security, at its most basic, means "the state of being free from danger or threat." In cybersecurity, well, good luck with that. Companies will never be free of cyberthreats as long as they operate in an interconnected world.

That doesn't mean you should give up shooting for that target. Attempting to achieve the unobtainable may go against "Goal Making 101," but it is important that organizations focus on security rather than mere compliance. Being compliant is a low bar—it simply means you are following the rules or regulations a law/rule-abiding entity must keep if it wishes to stay law/rule-abiding.

However, a recent study of 479 executives from mid- and large-sized companies across the United States found 47% of respondents were unsure what data compliance standards applied to their organizations.[1] This means that just under half of these executives had no way of knowing if they were compliant with cybersecurity standards and regulations such as those required for credit card data holders, health care organizations, or defense contractors. This is a big problem because not understanding the laws under which your organization must operate opens you up to a threat as pervasive as hackers: regulators.

While compliance generally allows you to avoid the threat of regulators, it is a long way from stopping the ne'er-do-wells cited and quoted in this report. In fact, one could argue that merely being compliant with an industry standard makes it easier for hackers to steal your data. You have given cyber-criminals the outline of your data frontier; they know how high the wall, how deep the moat.

Don't give that away. Be more than compliant. Shoot for finding the right types of personnel, structures, systems, and defenses you need to keep your data secure. Only then will your organization find itself more resistant to the threat posed by hackers … and regulators.

Data

Finally, many organizations focus on securing their systems when what they really want to do is secure their *data*. This is a critical distinction. A system compromise isn't a cybersecurity concern; after all, systems go down all the time for non-nefarious reasons. What organizations care about is what happens to their data.

[1] Liaison Technologies, 2016 State of Compliance, November 2016

Think of it like ye olde castle-keep. Kings and queens didn't want to protect the stones in their walls, they wanted to protect the jewels and heartbeats that lay within their confines. Same holds true for cybersecurity—it's what's inside that counts.

This distinction is important because when an organization is examining how to protect against cyberthreats, it often stops at the computer systems or database upon which the data resides. This is a crucial mistake—keep going! Don't forget that data are mobile. If it's important to you, your customers, or the government, it needs to be protected at all times—while at rest and while in motion. Focusing on system security runs the risk of having the data susceptible as soon as it leaves the refuge of the system.

To secure data, your organization must understand which information truly needs securing and must ensure it is protected while at rest and while in transit.

Security planners must understand the benefits and other implications of encryption. Encrypting data requires more storage space and more computer memory. It will also very likely impact the ease and productivity with which employees can view, use, and share that data.

Therefore, planners considering encryption must examine where, when, and how to use it to secure the data they believe is the most important to the organization (for example, intellectual property, personally identifiable information, credit card numbers, and personal healthcare information). Candidly, you must be prepared to ask questions that will produce answers you did not want. But, again, there is little room for wants in cybersecurity planning, it is all about needs.

Fail to Plan—Plan to Fail

Every organization should be prepared for a cybersecurity situation—simple system downtime, a regulatory issue, or a full-on criminal penetration. Planning your cybersecurity responses and defenses is the necessary first step to ensuring your organization can not only react to those situations but survive them.

Throughout this report, you have seen examples of the thoroughness and professionalism with which hackers—good and bad—operate. They are methodic. They are surgical. They are dedicated. They are legion.

Without a formal plan, an organization has no way through the morass of terrors that operating in cyberspace brings. So start planning.

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.

THE FINAL WORD

Reading through the results of our first Black Report survey, I couldn't help but think about the state of security software development today.

The fact is, security vendors are focused on building products that cater only to the security professionals who will use them. Features and functionality are based on customer feedback. Many vendors are simply out of touch with the latest attack techniques and have no idea about the motivations and experiences of the attackers themselves. I wonder what kind of insight we'd glean if we paid a little more attention to the attackers rather than just accepting the stereotypes we see in the media.

Regardless, this research underscored for me just how much vendors focus on their users' wants, not their needs. Steve Jobs famously said "A lot of times, people don't know what they want until you show it to them." Cybersecurity customers depend on vendors to include the features and capabilities that will help them succeed, whether or not they know what those features are.

Know Your Enemy

The main reason organizations invest in a security product is to protect themselves—their data, infrastructure, people, and customers. That's part of what inspired this study, to gain and share intelligence that will help answer the challenge posed by attackers who know no constraints and who remain several steps ahead of the curve. How else would we know that:

- Endpoint security is the countermeasure that presents the greatest challenge to hackers during a penetration test.
- Most hackers change their attack methodologies fairly often; 50% adjust them for every engagement.
- A large majority of hackers can find and exfiltrate targeted data on average in less than 12 hours after their initial breach.

Using intelligence about the enemy is a centuries-old concept. Sun Tzu wrote "If you know the enemy and know yourself, you need not fear the result of a hundred battles."

Why do we so easily disregard this wisdom? It's incumbent on us—security software vendors and practitioners—to continually feed the intelligence we glean and results of our investigations, incident responses, and breach debriefs into the tools that are available to help defeat cybercrime.

It's our duty to understand the real-life threat landscape. Without this critical feedback loop, there's no way we'll be able to address real-life use cases, protect against the latest threats, or adapt to the latest attack techniques.

Therein lies the beauty of this report. It comes straight from the practitioners and people who know how best to bypass defenses and make off with organizations' critical value data. Their feedback and expertise is a critical and often missing, component of the industry's product development strategies.

Without it, we are doomed to repeat the same failures we've experienced for years.

Dr. Jim Kent — Global Head of Security & Intelligence, Nuix

Jim is a global industry leader in information security, incident response, eDiscovery, and digital forensics. He has more than 20 years of experience as a senior digital forensics investigator, information security consultant, high-technology crime detective, and high-level advisor to law enforcement, government, financial, and commercial organizations.

Nuix

Nuix protects, informs, and empowers society in the knowledge age. Leading organizations around the world turn to Nuix when they need fast, accurate answers for investigation, cybersecurity incident response, insider threats, litigation, regulation, privacy, risk management, and other essential challenges.

Nuix makes small work of big data volumes and complex file formats. Our solutions combine advanced technology with the extensive knowledge of our global team of industry experts. We bring data to life with clarity and intelligence to solve critical business problems, reduce crime, and secure and manage information.

nuix.com

North America
USA: +1 877 470 6849

» Email: sales@nuix.com

EMEA
UK: +44 203 786 3160

» Web: nuix.com

APAC
Australia: +61 2 9280 0699

» Twitter: @nuix

nuix
Simple. Powerful. Precise.