eSENTIRE®

Know Your Enemy. Know Your Risk.

A report on sensitive data security.

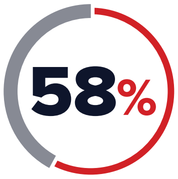
Executive Summary

Theft of sensitive data, ranging from employee and customer information to intellectual property, remains at the epicenter of the battle between threat actors and the organizations responsible for protection. Consumers and businesses are sharing more data across an ever-expanding digital landscape, including cloud, mobile and IoT. So, organizations are increasingly challenged with the delicate balance of data use versus associated risk.

Recent data breaches involving Facebook, Equifax and Marriott demonstrate no organization is immune to risky security practices. However, the consequences incurred by organizations at this scale are a misrepresentation of what small and medium-sized businesses (SMBs) can potentially face. Armed with massive financial resources, insurance policies, political lobbyists and more, large enterprises have the time, resources and resilience to survive a sensitive data breach. On he other hand, SMBs are faced with an ultimatum: evolve or perish. Unfortunately, evolution at the speed necessary for SMBs to stay competitive requires weighing potential business success vs. business risk. While risk is unavoidable, a sensitive data breach does not have to be.

WIth the intention of helping SMBs better protect their sensitive data, this white paper explores:

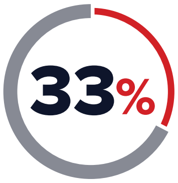
- Know Your Enemy: A hacker’s mindset, motivations and tactics
- Know Your Risk: Probability of an incident and financial risk
- What’s working, what’s not and making the case for future-proof protection



of SMBs reported a data breach over the past 12 months*

$1.43M

is the average cost of the damage or theft of IT assets for SMBs due to a breach*



year-over-year increase in the cost of data breaches for SMBs*

*Ponemon: 2018 State of Cybersecurity in Small & Medium Sized Businesses

Know Your Enemy

"Know your enemy" is one of the oldest military strategy concepts. You must understand how and why you will be attacked in order to defend sensitive data. The "why" for theft of sensitive data may seem rooted in financial motivation. However, industry studies and interviews with hackers point to motivations other than monetary gain[1] :

- I like the challenge to learn: **86%**
- I hack for the luz (fun, laughter or amusement, especially that derived at another's expense): **35%**
- I hack for financial gain: **21%**
- I hack for political or social motives: **6%**

Of these respondents, 46 percent agree that life with no danger would be too dull for them and 64 percent of respondents say they enjoy taking the risks associated[2].

Additionally, many hackers indicate that the greater the sensitivity of the data, the greater the potential for entrance to social groups or elevated status within these groups. In fact, sensitive data is looked at as a trophy or proof of a hacker's skillset and success. While the risk of prosecution is recognized, 77 percent of hackers say their presence is rarely, if ever, identified during an attack. Even more concerning, 90 percent of respondents indicate that they can cover their tracks after a breach in less than 30 minutes, further reducing their risk[3].

While there are numerous behavioral studies on criminal theory that can dissect a hacker's motivations, the key is to think of it from their perspective. If the potential benefit outweighs the risk, theory indicates that people, whether they are a hacker or not, will engage in criminal activity. As a result, SMBs must look at the sensitive data they protect and answer the following from a hacker's perspective:

- What is the data worth from a social perspective?
- What is the data worth from a financial perspective?
- What is the ease of obtaining the data?
- What is the risk of being caught?
- What are the consequences of being caught?

[1,2,3] 2018 Nuix Black report

Inside the mind of a hacker

Knowing your enemy's mindset is valuable. Knowing how they will attack is invaluable. In this section, we will "know our enemy" by exploring the mind of an attacker leveraging eSentire's Red Team, a group of best-in-class, ethical hackers who utilize the most deceptive methods to test client defenses. There are countless ways an attacker could gain access to sensitive data. We will cover an example method to demonstrate how an attacker could gain access to sensitive data without using malware, and in this case, even use sensitive data from other breaches against a targeted organization.

Gathering information

A hacker's version of knowing their enemy is reconnaissance or more commonly referred to in the security community as Open Source Intelligence (OSINT). OSINT is a technical term for collecting publicly available information on a target. While not necessarily technical in nature, the reconnaissance stage is foundational to determining the right methods and tools to quickly and covertly achieve objectives.

The reconnaissance stage of an attack can be thought of like an iceberg. The hacker's intrusion activity to find and exfiltrate sensitive data is just the tip of the iceberg. But, the information gathering, social engineering and planning that takes place prior makes up everything unknown to the target organizations and beneath the surface. This also is an example of the first-mover advantage that hackers often hold over their targets. By the time the reconnaissance stage is complete, the adversary is in an advantageous position to attack with knowledge of defensive infrastructure and weaknesses.

> The most important and often overlooked stage is information-gathering … the more time you spend on reconnaissance, the more options you have to make a hack successful.

Know Your Risk

Knowing your enemy is critical to understanding why your sensitive data is being targeted. And, knowing the risk associated with loss of that data is key to prioritizing protection.

While what constitutes sensitive data appears to be self-explanatory, classification based on an organizationally accepted definition is not widely adopted in the SMB space. In a recent survey conducted by eSentire targeting 300 security professionals, 63 percent of organizations had not clearly defined what sensitive data was in the context of their organization. Of those respondents, 55 percent lacked a formalized data classification policy and only 51 percent felt confident they had the ability to detect and respond to a targeted sensitive data attack.

“

The first step of reconnaissance is to look at the target’s infrastructure. We look for servers, DNS and any exposed services that are accessible to anyone on the internet.

For this attack, the identified password reset tool required four pieces of information: username, date of birth, last four digits of social security number and the answer to a customized security question, which in this instance was the place of birth of the employee. Here is how eSentire’s Red Team cracked the password reset tool:

Step 1: Identify the user and username (OSINT)

“The first step was to identify a particular employee that we could leverage this password reset tool against and try to find these four pieces of information from this employee. We settled on a particular employee who had a very unique name. Obviously, the more common a name, the more difficult it is to narrow down specifically who you are looking for.”

Once the target’s name is identified, discovering what the username is a simple process. There are several free scraping applications online that can discern usernames and emails with a very high degree of certainty. It is usually some kind of first name and last name convention (johnsmith, john.smith, john_smith, etc.).

Step 2: Date of birth (OSINT)

“Second piece of information … date of birth. This is actually easier to get than you might imagine. There’s a ton of perfectly legitimate ‘look up this person,’ ‘check to see if a person has a criminal record’ and similar websites. Some of them are behind a paywall … if you want to pay for access to this kind of information, you can. However, a lot have free versions as part of a trial. If you collect pieces of information from a number of these websites, you can deduce certain things. You can build a highly detailed profile of someone without spending a dime.”

Step 3: Social security number (Dark Web)

“The last four digits of the social security number are a little bit trickier to get … I should say trickier from an open-source perspective. In this case, we quickly found this information on the Dark Web.”

Data breaches happen on a daily basis. Emails, passwords, credit card numbers, social security numbers and more are compromised and made available. Bad actors try to monetize this stolen data on marketplaces hosted on the Dark Web and release information for free to demonstrate their capabilities for hire. If hackers are unsuccessful discovering intelligence on their own accord, chances are pretty good it is available for purchase on the Dark Web.

Step 4: Place of birth (social media)

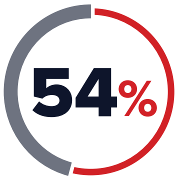
“The final piece of information. The place of birth. This was the most difficult to discern because the place of birth can be very different from a person’s address. A person can be “from” Philadelphia, but they were actually born in Oregon or a different country perhaps. This is where we really leveraged social media. We dug into their Twitter and Facebook profiles and started to notice a trend. We noticed a lot of support for a particular local college sports team and a lot of support for local small town events. Then we looked up where the closest hospital was to this particular community and what city it was in and went with that. Now at this point, we’re just making a guess. An educated guess, but still a guess. It happened to be right.”

Step 5: Setting up lateral movement

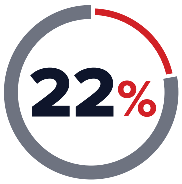
“Once we were in, we eventually got access to their active directory in an attempt to compromise other accounts. We pulled a list of user names … several thousands of them. The great thing about hacking is people are generally people of pattern. This is where brute force comes into play.”

A brute force attack is a classic technique. It typically leverages a program that automates thousands or millions of login attempts with varying usernames and passwords. As a security countermeasure to brute force attacks, many login applications will lock out an account after a handful of failed login attempts in a relatively short amount of time. Still, a savvy attacker can use brute force in a more strategic way that does not trip any security rules.

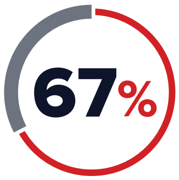
Users tend to leverage the same passwords for everything because nobody wants to remember dozens of different passwords. As a response to this, most companies mandate that users change passwords every 60 to 90 days or so. This makes sense as a security measure, as a constantly changing repository of passwords within a network makes it more difficult for hackers. However, this common mandate has led to the proliferation of common password templates. Nobody wants to memorize a brand new password every few months, so they opt to memorize a template instead. Thus, spring2019, summer2019, winter2019, etc. Password management solutions do exist but have yet to achieve widespread adoption.



of organizations lack visibility into password practices**



of organizations require employees to use a password management solution**



of organizations cited weak passwords as a pain point**

“So, we were doing this exercise in July of 2017. We brute forced two passwords, *summer2017* and *summer17* and sure enough, out of several thousand emails we were able to get access to 39 accounts.”

With control of over 40 total accounts now (39 plus the originally compromised account), the eSentire Red Team was able to move laterally in the network with little impediment. Sensitive data such as customer lists, documents pertaining to fiscal year planning and strategy and executive credit card information were eventually discovered.

** Ponemon “2018 State of Cybersecurity in Small & Medium Sized Businesses”

Inside the mind of a hacker

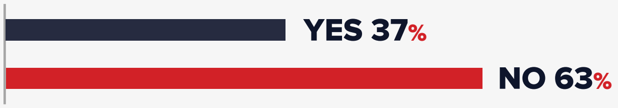
Gathering information

Knowing your enemy is critical to understanding why your sensitive data is being targeted. And, knowing the risk associated with loss of that data is key to prioritizing protection.

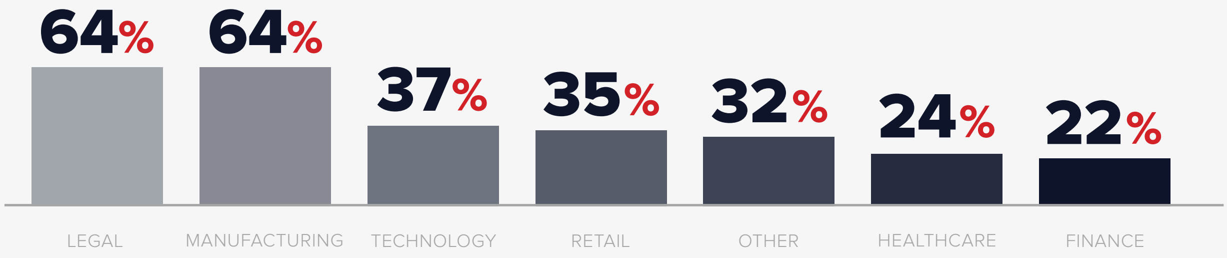
While what constitutes sensitive data appears to be self-explanatory, classification based on an organizationally accepted definition is not widely adopted in the SMB space. In a recent survey conducted by eSentire targeting 300 security professionals, 63 percent of organizations had not clearly defined what sensitive data was in the context of their organization. Of those respondents, 55 percent lacked a formalized data classification policy, and only 51 percent felt confident they had the ability to detect and respond to a targeted sensitive data attack.

Is sensitive and/or crown jewel data clearly defined at your organization?

No and unsure responses combined

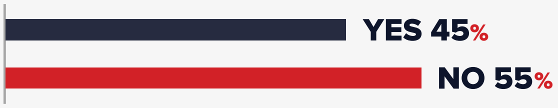


Percent of respondents who did not have sensitive/crown jewel data clearly defined

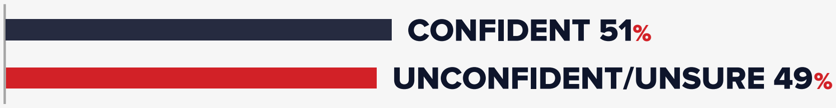


Does your organization have a data classification policy?

No and unsure responses combined



How confident are you in your organization's ability to detect and respond to a targeted attack on your sensitive data?



-eSentire Survey of 300 North American IT Security Professionals, May 2019

Sensitive data can take many forms. Understanding the associated financial risk can help organizations to identify and classify their sensitive data according to risk tolerance.

Financial risk of sensitive data

Cybercriminals and the economy in which they conduct business live in the shadows, making it difficult to quantify the exact cost of sensitive data theft to the global economy. The average cost of a data breach is $3.86 million, according to The 2018 Cost of Data Breach Study by Ponemon. In 2017, the IP Commission on the Theft of American Intellectual Property estimated damage ranging between $225 and $600 billion annually, with both figures trending up from their previous respective reporting. While these statistics are a powerful representation of just how big the economy for sensitive data theft is, it is not specific to SMBs.

To understand the financial risk of your organization's sensitive data, you must know the probability of an attack and the potential loss specific to your organization.

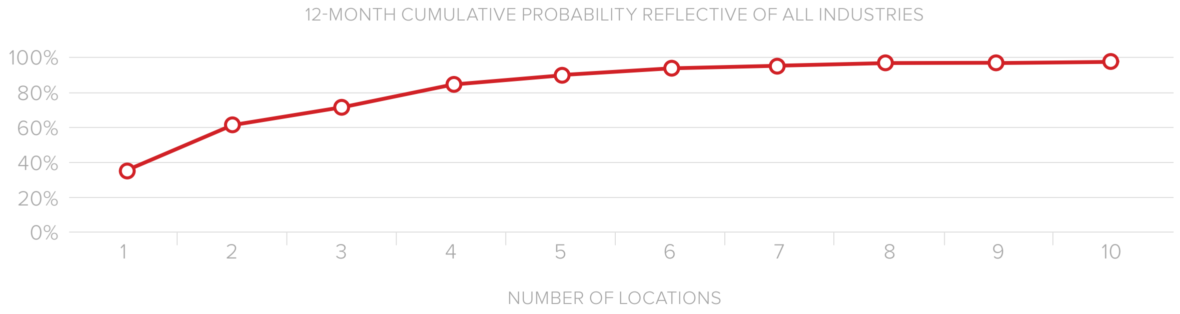
⚠ **RISK = PROBABILITY X POTENTIAL LOSS**

Probability

It's not if, but when. Every security practitioner has seen this slogan meant to instill fear, uncertainty and doubt, at some point. However, how is it relevant to your organization? On a long enough timeline the probability of avoiding a breach for any organization, regardless of adequate defensive measures and resources eventually reaches zero. The question is what is your organization's contextual risk in today's landscape and what is the probability of an incident due to a bypass of your existing preventative controls?

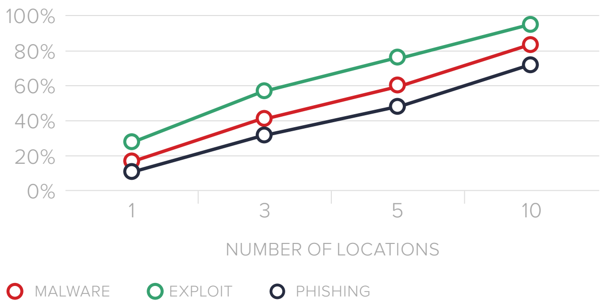
Look at the past to help predict the future. In an effort to help organizations determine their risk over a 12-month period, eSentire used its Security Operations Center (SOC) data reflective of 650 organizations spread over more than 50 countries. The data was used to determine future probabilities contextual to number of locations protected and the industry in which an organization operates. Propensity modeling produced cumulative probabilities of at least one incident that would bypass an organization's existing controls over a calendar year. The charts below reflect a sampling to see where your organization's probability aligns correlative to phishing, malicious code, known exploits and overall cumulative probability:

GLOBAL COMPOUNDED RISK OF AN INCIDENT DUE TO A BYPASS OF PREVENTATIVE MEASURES



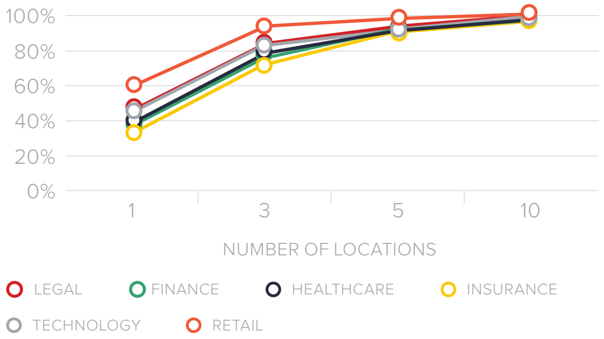
GLOBAL COMPOUNDED RISK OF AN INCIDENT DUE TO A BYPASS OF PREVENTATIVE MEASURES BY ATTACK METHOD

12-MONTH CUMULATIVE PROBABILITY BYNUMBER OF LOCATIONS



COMPOUNDED RISK OF AN INCIDENT DUE TO A BYPASS OF PREVENTATIVE MEASURES BY INDUSTRY

12-MONTH CUMULATIVE PROBABILITY BY NUMBER OF LOCATIONS



Cost of sensitive data

While the charts above serve to fill part of the risk equation, organizations must also determine the potential cost of losing sensitive data. As part of Ponemon's 2018 Cost of a Data Breach study, per capita cost of sensitive records lost were calculated based on:

- Detection and escalation costs
- Post data breach response costs
- Notification costs
- Lost business costs

The subsequent per capita cost of a single record per industry was determined in USD to be:

- Healthcare: **$408**
- Financial: **$206**
- Services: **$181**
- Pharma: **$174**
- Technology: **$170**
- Energy: **$167**
- Education: **$166**
- Industrial: **$152**
- Entertainment: **$145**
- Consumer: **$140**
- Media: **$134**
- Transportation: **$128**
- Communication: **$128**
- Hospitality: **$120**
- Retail: **$116**
- Research: **$92**
- Public: **$75**

To determine your financial risk, use the following equation:

Probability (39 percent for healthcare with one location as an example) x ($408 per record x number of sensitive records you have)

In this case, if your organization's data classification policy determines 10,000 records as sensitive, your financial risk profile would be $1,591,200 USD.

Please note, this does assume that the incident incurred results in a loss of sensitive data. While most incidents do not involve sensitive data loss, organizations determining risk must account for worst case scenarios. In the event an incident does involve sensitive data loss, the total financial risk should serve your security team, and more importantly your decision makers and the Board, in determining if the security function is appropriately invested to offset risk to an acceptable level.

Conclusion

Know your enemy and know your risk are two fundamental steps in protecting your organization's sensitive data.

Identifying the data that represents the greatest potential loss if it were stolen or compromised is the first step to determining risk. A formal data classification policy that clearly identifies these assets is fundamental to your cyber risk management strategy. If your organization lacks the resources or expertise to implement such a policy, ongoing advisory or virtual CISO services are a viable solution to help your organization understand its contextual financial risk profile.

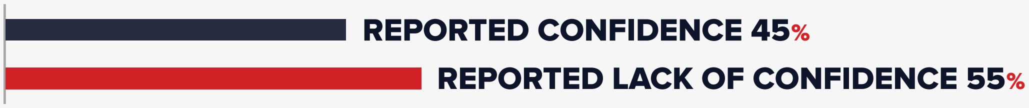
As the eSentire Red Team and SOC propensity model demonstrate, the probability of a breach remains at unacceptable levels. Skilled hackers can evade perimeter and internal security measures with relative ease. The primary tool used to achieve objectives was not customized malware or a zero-day exploit, but rather personal data and social engineering. While relatively simple, these techniques and methods are extremely effective in targeted attacks. Furthermore, as long as hackers are incentivized based on social acceptance and financial gain, they will continue to target sensitive data. And, as data continues to proliferate across cloud, mobile and IoT, organizations will continue to be faced with an increasing security risk.

> Prevention is futile unless it's tied to detection and response.
>
> — Gartner Analyst quote

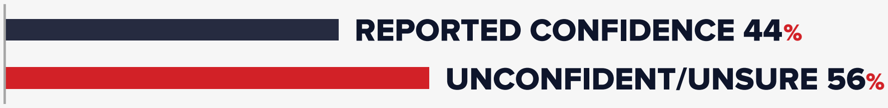
Evidenced in daily breach headlines, organizations are losing ground to the evolving threat landscape and as a result, complementing their existing preventive measures with outsourced Managed Detection and Response (MDR). Intrusions like the one described in this report are inevitable. How quickly organizations can detect and respond to these attacks is the most important factor in risk mitigation. More specifically, the ability to identify and contain an attacker's lateral movement and attempts to exfiltrate sensitive data is a necessity to avoid business disruption.

SMBs are still catching up to this paradigm shift. eSentire's research indicates there is a collective lack of confidence that security teams have adequate ability to detect, respond and contain threats in a timely fashion.

Assume an attacker has bypassed your perimeter. How would you describe your confidence level in your organization's ability to detect lateral movement in your network?

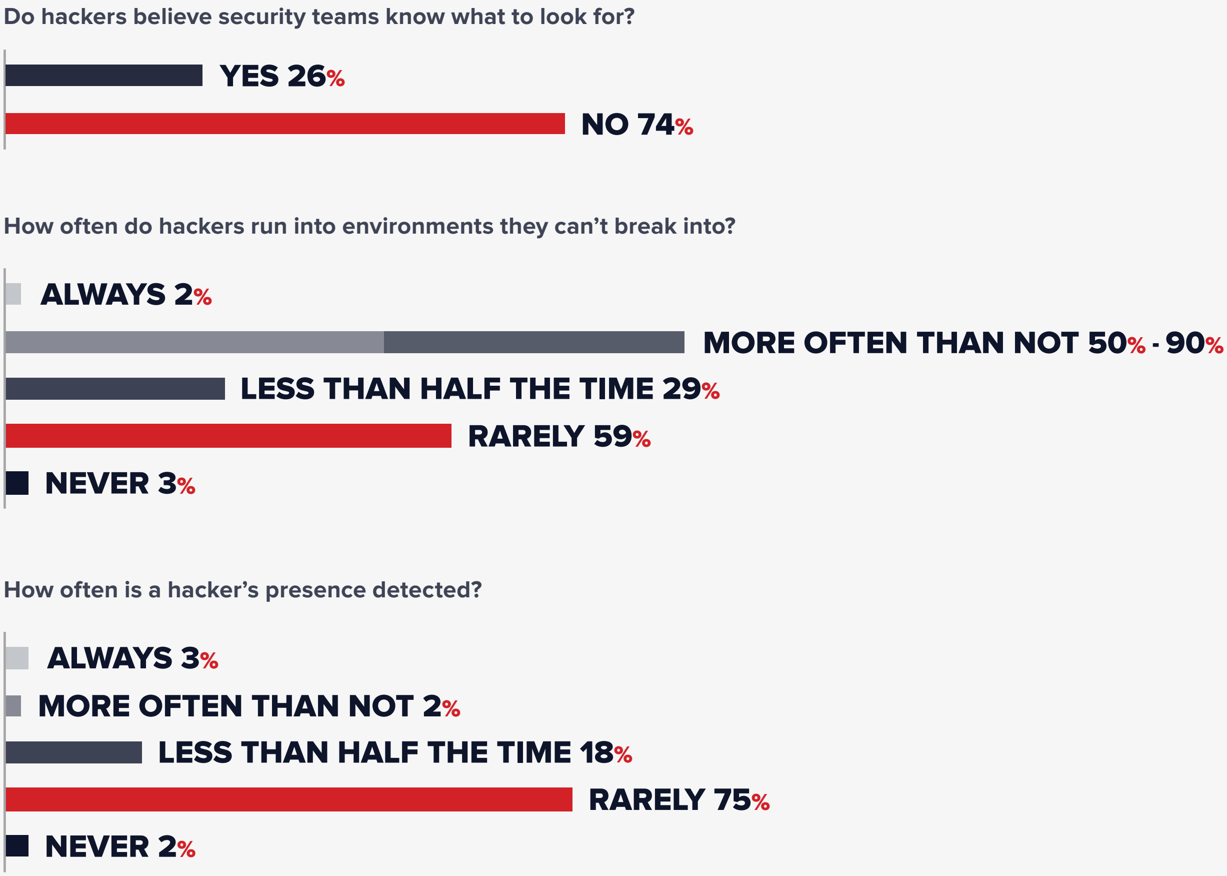


Assume an attacker has bypassed your perimeter. How would you describe your confidence level in your organization's ability to respond and contain lateral movement in your network?



-eSentire Survey of 300 North American IT Security Professionals, May 2019

While a majority of SMBs lack confidence in their ability to detect and respond, data from the 2018 Black Report highlights extreme confidence in an attacker's ability to evade detection and achieve their objectives.



Do hackers believe security teams know what to look for?

How often do hackers run into environments they can't break into?

How often is a hacker's presence detected?

Source: The Black Report: Decoding the Minds of Hackers 2018

Armed with ample time and resources to accomplish their objectives hackers will always hold the first-mover advantage. Organizations must consider the financial risk related to their sensitive data and subsequent gaps that must be filled to mitigate unacceptable levels of risk.

For most SMBs, protecting sensitive data requires additional investment in detection and response capabilities. Investment in the people, process and technology necessary to leverage a Security Operations Center (SOC) can be a sizable commitment that many SMBs are not prepared to make. For organizations that lack the expertise or budget necessary to build an internal SOC, Managed Detection and Response (MDR) services are a viable alternative to complement an existing security team's capabilities.

eSENTIRE®

eSentire, the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $5.7 trillion AUM in the financial sector alone, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.esentire.com** and follow **@eSentire.**