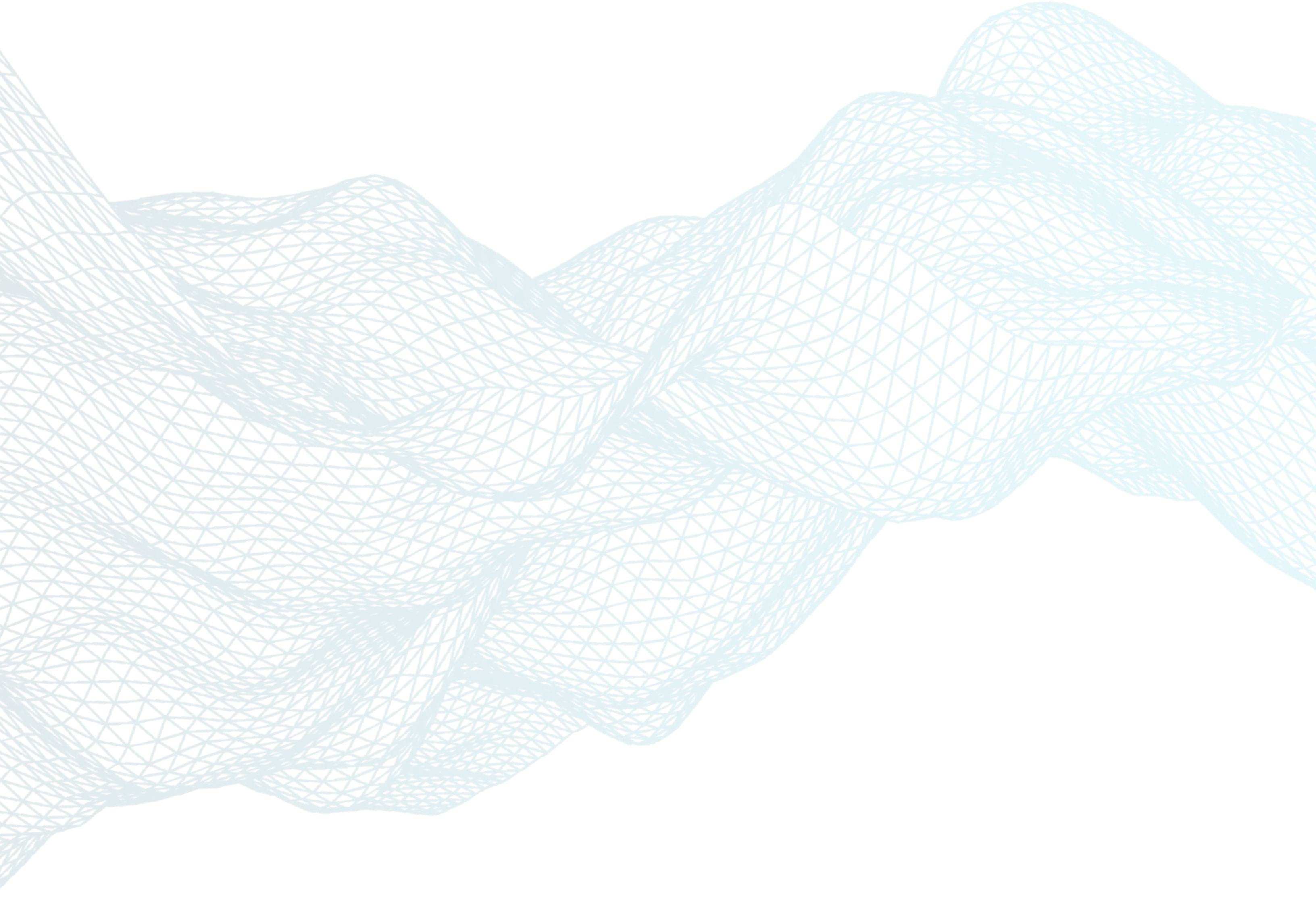
eSENTIRE

WHITE PAPER

Put Your Cyber Defenses to the Test

Identifying which proactive risk management programs meet your organization's needs to manage cyber risk and safeguard your sensitive data



Introduction

Today's cybercrime gangs are sophisticated organizations with access to significant funds and an ecosystem of specialized tools and services. The ever-expanding and increasingly complex IT environment of modern enterprises, plus generally poor cybersecurity hygiene and training, creates a world of opportunity for attackers.

All too often, the story ends with a chaotic response that actually made the situation worse and amplified repercussions from customers, insurers, the market, and regulators. A 2021 penetration testing research survey, commissioned by eSentire, showed that it can take 20 hours, on average, for a penetration tester to simulate a successful data breach:

- 6 hours to breach the perimeter
- 7 hours to locate and gain access to sensitive data
- 7 hours to exfiltrate the data

The survey also looked at the total breach time by industry and found that it took penetration testers 11 hours to breach industries such as retail, sports & entertainment, and transportation. On the other hand, it took penetration testers 13 hours on average to breach the financial services, manufacturing, government agencies, and telecommunications/technology sectors.

Question 1: On average, how long does it take to complete each of the following milestones during a simulated attack?

Exfiltrate the data	7hrs
Locate and gain access to targeted data	7hrs
Breach the perimeter	6hrs

Question 2: On average, how long does it take to complete a breach (breach the perimeter, identify critical value assets, and exfiltrate the data) for each of the following industries?

13hrs	12hrs	11hrs
Financial Services Manufacturing/Industrial Municipal/State Gov. Telecom/Tech	Education Construction Energy & Utilities Pharmaceutical Food & Beverage Hospitality Hospitals/Healthcare Information Law/Legal Real Estate	Retail Sports & Entertainment Transportation

Additional key findings include:

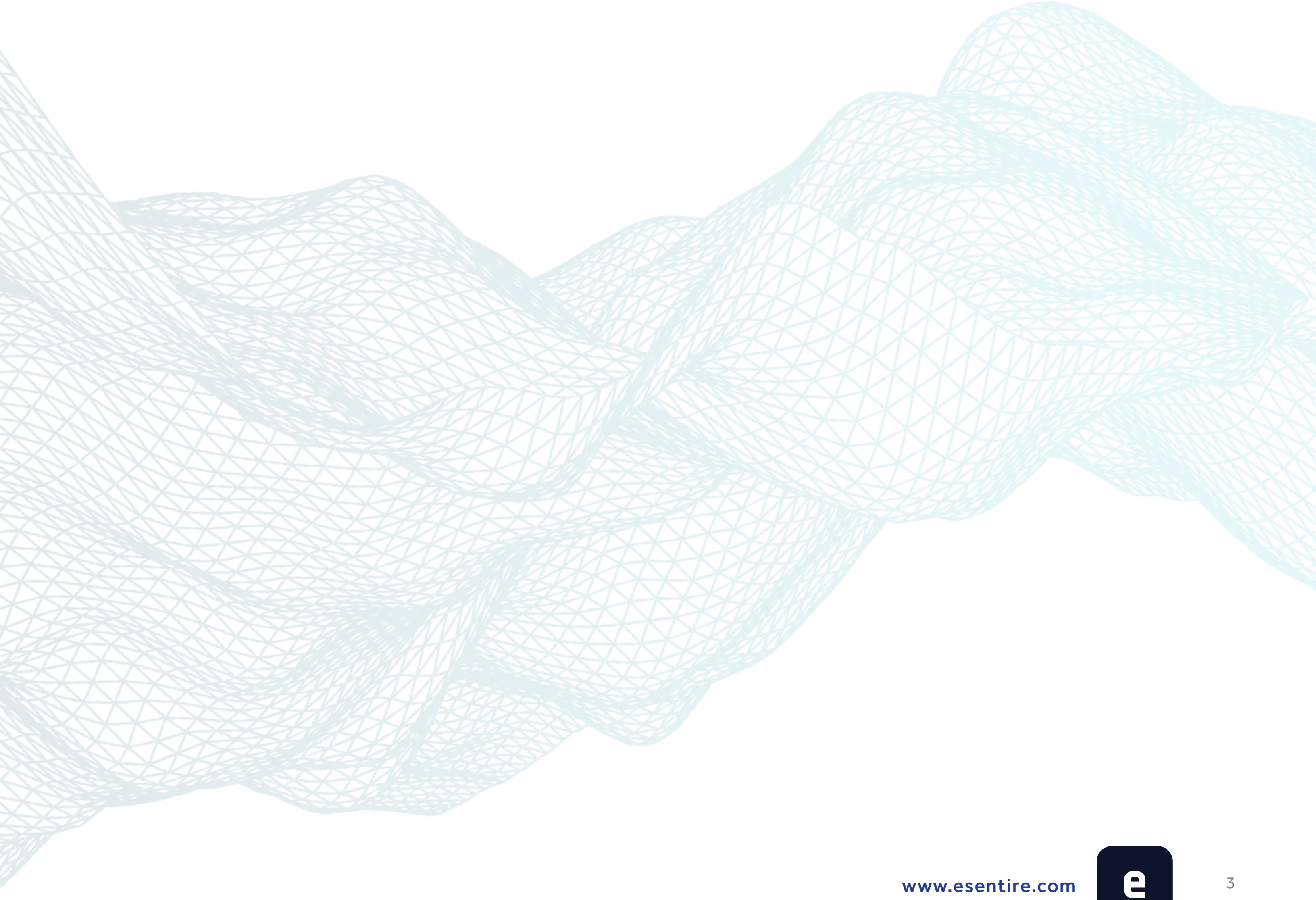
- Only 39% of organizations have the detection & response capabilities needed to deter an attacker.
- While the most successful attack methods include the use of malware from a cost-to-benefit perspective, social engineering tactics, especially phishing, were used most frequently to launch a cyberattack.
- Only a little over 50% of organizations can successfully stop an attacker at each of the key breach milestone.
- On average, it takes an attacker only 13 hours to complete a full breach and an additional 30 minutes to completely cover their tracks.
- Although 86% of IT teams know what to look for to detect a cyberattack, penetration testers believed they would be 68% more successful in their test attacks if they used unethical or unrestricted methods similar to those used by real-world adversaries.

Sensitive data—especially credentials, PII, and PHI—has considerable value for cybercriminals, who sell it in online marketplaces and use it to further their activities. No matter how large or small your organization is, threat actors are going to exploit vulnerable systems and take advantage of human error in pursuit of their objectives.

Managing these risks by continuously testing your organization's cyber defenses is essential to maintaining operations and delivering services. In this white paper, we discuss the means, motives, and opportunity of why threat actors deploy cyberattacks against organizations, the most common attack vectors most organizations are vulnerable against, and how you can put your cyber defenses to the test to manage your cyber risk and safeguard your sensitive data.

Research Methodology

In May 2021, eSentire engaged an external research firm to conduct a 7-minute online survey among 200 individuals who are involved with penetration testing for other companies. The overall research objectives included profiling the experiences of penetration testers, quantifying the risks of a potential breach at the organization they provide services for, and estimating the time required to detect, isolate, and respond to a potential incident.



Understanding Cyber Threats: Means

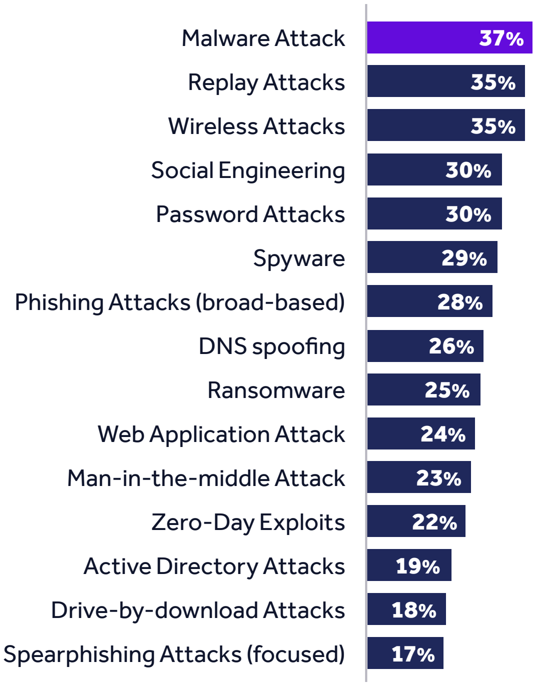
The variety of options at the threat actor's disposal is the product of a world of opportunity when it comes to launching an attack.

Penetration testers, like real-world attackers, use various cyber threats as part of their engagement to test their clients' cyber defenses and our 2021 penetration testing survey showed that the top three types of cyberattacks proven to be most successful from a cost-to-benefit ratio were malware attacks (37%), replay attacks (35%), and wireless attacks (35%).

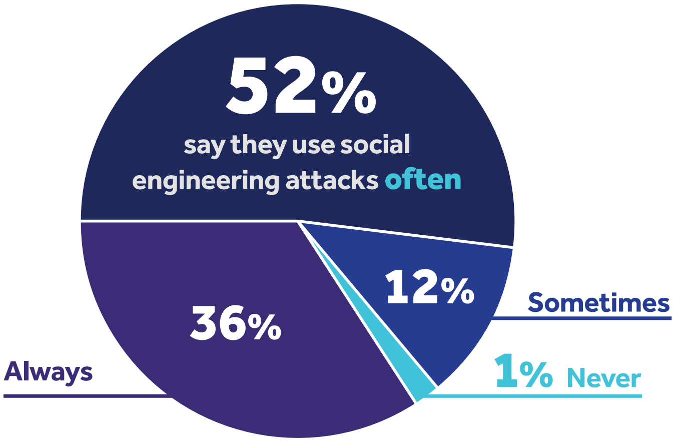
However, regardless of the industry, many cyberattacks begin with a phishing email that tricks a user into helping the attacker. The same survey also showed that experienced penetration testers used social engineering tactics to obtain information about a target organization.

Out of all the social engineering tactics used, phishing was the tactic that's most likely to succeed (39%).

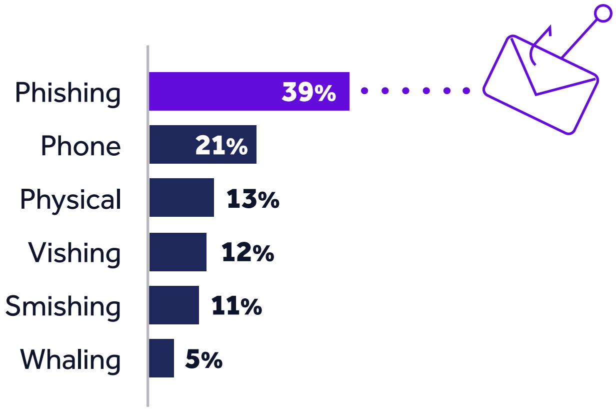
Question 3: On a free form engagement, which type of attack is most likely to succeed from a cost/return perspective?



Question 4: How often do you use social engineering to obtain information about a target?



Question 5: What type of social engineering attack is most likely to succeed?



While ransomware attacks used to be opportunistic, today we see sophisticated operations that target high-value victims and combine automated elements with manual activities.[1] In fact, cybercriminals are rapidly evolving their Tactics, Techniques, and Procedures (TTPs) and leveraging role specialization to expand the reach and velocity of their campaigns.

What's more, the emergence of ransomware-as-a-service and affiliate models have made it even easier for new operators to break into the cybercrime market.[2] Research commissioned by eSentire also revealed:

55%
Organizations that were able to successfully detect a penetration test and prevent a breach.

13hrs
Time it can take for an attacker to breach the perimeter, gain access to targeted data, and exfiltrate the data, on average.

30mins
Time it can take for an attacker to cover their tracks after successfully gaining access into an organization's environment, on average.

Unfortunately, while most companies provide some form of annual cybersecurity awareness training to reduce the likelihood of employees being hooked by phishers, most programs focus on overly simplistic lures. Taken from public events, these generic examples don't capture the real danger that comes from targeted cyberattack campaigns.

They also tend to rely on disengaged metrics like employee attendance and simple test results as a proxy to measure business risk reduction—creating a false sense of security which only further exposes the business to cyber risk.

In today's threat landscape, security leaders should recognize that a one-time or once-per-year training exercise for their employees isn't enough. After all, it only takes one successful social engineering or business email compromise (BEC) attempt to gain initial access into your environment that can lead to a business disrupting event.

[1] For an illustrative example of a hands-on-keyboard ransomware attack, see Defending Against Modern Ransomware: Lessons from the SunWalker Incident [eSentire]
[2] You can learn more about these developments in Dissecting Today's Ransomware Ecosystem Ransomware-As-A-Service, Targeted Intrusions and Opportunistic Attacks [eSentire]

Understanding Cyber Threats: Motive

Cyberattacks targeting sensitive data are widespread simply because that data is valuable to their operations both as a revenue source and as a direct enabler of malicious actions.

First, using ransomware to encrypt crucial data continues to generate impressive returns for cybercrime gangs, with the average ransom across all industries reaching $570,000 in the first half of 2021—an 83% increase over 2020.[3] Attackers routinely employ double- and triple-extortion tactics to compel their targets to pay not just to recover access to systems but also to prevent the release of stolen sensitive data, avoid the possible regulatory fines that may result, and keep the event out of the public's eye.

Second, regardless of whether the victim pays the ransom, cybercriminals may sell the stolen data on the Dark Web and use the profits to advance their own activities:

- Credentials are especially valuable for gaining initial access into and performing intrusion activities within an IT environment.
- Financial information is used to compromise bank accounts and commit wire fraud.
- PHI can be used to blackmail individuals since it's regarded as being much more valuable than credit card information, with each record worth upwards of $1,000.[4]

The profits also serve as fuel in the engine of cybercrime, self-funding additional extensive operations and ongoing research into new ways to victimize organizations. Ultimately, leveraging this ecosystem of experts and ransomware-as-a-service reduces operational costs and accelerates the criminals' time-to-market, while greater success rates lead to growing ransom amounts generates ever increasing revenue.

Understanding the cyber threats targeting sensitive data is an essential element of managing the associated cyber risk. As organized cybercrime continues to evolve, the combination of motive, means, and opportunity has created a self-reinforcing ecosystem in which stolen data plays a key role.

Verizon's 2021 Data Breach Investigations Report (DBIR) shows that the financial motive is behind roughly **95%** of all breaches.[5]

According to IBM's Cost of a Data Breach Report 2021, the average cost of a breach rose 10% from 2020 to 2021, reaching **$4.24M** USD.[6]

Dark Reading reported that the average ransom across all industries reached $570,000 in the first half of 2021—an **83%** increase over 2020.[3]

[3] See Average Ransomware Payment Hits $570,000 in H1 2021 [Dark Reading]

[4] See Why hospitals and healthcare organizations need to take cybersecurity more seriously [The Brookings Institution]

[5] 2021 Data Breach Investigations Report [Verizon Business]

[6] Cost of a Data Breach Report 2021 [IBM]

Understanding Cyber Threats: Opportunity

The unfortunate reality is that attackers have no shortage of attack vectors, due to a combination of factors.

1 On-premises applications and services have moved to the cloud, IT and OT (Operational Technology) have intersected, the Industrial Internet of Things (IIoT) has arrived, and dedicated workstations have been substituted for laptops and mobile devices—with bring your own device (BYOD) policies supplying many of the endpoints. In addition, shadow IT systems (e.g., those that are used but not officially sanctioned) are an ever-present problem that have likely increased due to the widespread adoption of remote work.

2 Recent years have seen an increase in the number and impact of zero-day exploits observed in the wild. A threat actor equipped with a zero-day exploit is presented with a land of opportunity. Attacks can proceed for weeks or months before investigations uncover the new exploit and vulnerability, and only then can the vendor begin to develop a patch. For example, the ProxyLogon vulnerabilities within Microsoft Exchange led to tens of thousands of organizations being at significant risk of compromise.

3 One of the most common tenets of business is to outsource any supporting business functions to third parties or supply chain vendors so you can focus on your core competencies. This vast web of suppliers, partners, and service providers enjoy privileged access to customer-facing solutions, mission-critical IT environments, and sensitive data. However, the convenience, efficiency, scale, and other desired outcomes afforded by interdependence comes at a cost: third party and supply chain risk.

Sensitive data—especially credentials, PII, and PHI—has considerable value for cybercriminals, who sell it in online marketplaces and use it to further their activities. No matter how large or small your organization is, threat actors are going to exploit vulnerable systems and take advantage of human error in pursuit of their objectives.

Managing these risks by continuously testing your organization's cyber defenses is essential to maintaining operations and delivering services.

Put Your Cyber Defenses to the Test

Rather than learning the hard way about gaps in defenses and shortcomings in response plans, organizations should take proactive measures to identify and manage risk. At the same time, every organization is at a different stage in its cybersecurity journey: some are building a security function from the ground up, others are working to test and harden defenses against the most advanced threat actors, and most fall somewhere in-between.

Fortunately, there are several cyber risk management measures that can help your organization test your defensive posture and overall preparedness:

	Phishing and Security Awareness Training	Vulnerability Management	Penetration Testing	Red Team Engagements
What is it?	Context-relevant training to teach team members to recognize and report phishing attempts	Prioritize vulnerabilities that present the greatest potential risk and remediate against the most dangerous exploits first	Human-led methodical approach to breach the perimeter and acquire targeted data	White hat attack employing a full range of TTPs and extending over a longer period of time
Why do the engagement?	Build a culture resilient to one of the most common and effective attack techniques	Identify exposed and vulnerable systems to inform architecture and patch management	Determine the degree to which an attacker can gain access to your IT environment	Determine weaknesses in security systems (including an organization's ability to detect and respond)

Consequently, understanding the purpose of each service is essential to meeting business objectives and accounting for your organization's unique risk profile.

Phishing and Security Awareness Training (PSAT)

The IT environment is only one avenue for threat actors. Many cyberattacks begin with a phishing email that serves to deliver a malicious payload or to trick the recipient into handing over credentials or other useful information.

Unfortunately, while it's common practice to scapegoat employees for their mistakes or to act like phishing lures are easy to spot, the reality is that cybercriminals are extremely skilled at disguising their lures.

An effective PSAT program should emphasize building cyber resiliency by increasing risk awareness, rather than trying to turn everyone into security experts. To that end, look for a program that:

- ✓ Drives security awareness and behavioral change with user-specific training to reduce the risk of phishing-based intrusions
- ✓ Tests user resiliency by testing the user's ability to identify and avoid the latest phishing tactics and campaigns
- ✓ Identifies and measures improvement by identifying the high-risk users and groups on your team to reduce the risk associated with their privileges and access
- ✓ Alleviates resource constraints by automating testing and training, reducing the burden on your team
- ✓ Meets regulatory requirements by helping your security team comply with state, industry, and professional regulators and obligations

Vulnerability Management

Most IT teams are already overburdened. As a result, cybersecurity becomes reactive, rather than proactive, which means your IT security staff may spend most of their time responding to cyber threats as they are uncovered, rather than preventing them from occurring.

A comprehensive Vulnerability Management program helps to alleviate operational burdens and to improve security outcomes by combining three elements:

- ✓ Continuous awareness of the threat landscape (e.g., from advisories, notifications, cyber news, etc.)
- ✓ Vulnerability scanning to understand which systems are inadvertently exposed
- ✓ Disciplined, risk-based patch management

Penetration Testing

While a vulnerability scan tells you what systems are exposed, it won't tell you whether a threat actor can gain entry into your environment—and whether or not your existing defenses (technology and people) can detect the intrusion. In a pen test, a security professional actually tries to break into your environment—using many of the same Tactics, Techniques, and Procedures (TTPs) as real-world attackers. Often, the tester is pursuing a specific objective, like finding and exfiltrating sensitive data or gaining administrative rights on a domain controller.

However, while a pen test is a very useful mechanism for identifying gaps in your defenses, it's not truly representative of a real-world attack for a few reasons:

1. In most pen tests, your IT team is aware of the activity and is on the lookout for it
2. Penetration testers only use "ethical" attack methods
3. There's generally a time limit on the exercise

Red Team Engagements

Other than an actual real-world attack, a red team test is the most effective way to truly assess your security posture. It's a simulation of an advanced threat actor to test your organization's prevention, detection and response capabilities and is a more in-depth than a penetration test.

It combines various techniques to evade detection and prevention capabilities, including OSINT, phishing, wireless and covert physical and network attack tactics, techniques, and procedures (TTPs). However, unlike a penetration test:

- ✓ The time limit, if there is one, is measured in weeks or months
- ✓ The red team can use 'unethical' methods to test your defenses (e.g., turning to the Dark Web for resources)
- ✓ Only the key stakeholders of the target organization are aware of the engagement

The result is an attack that, for all intents and purposes, and to all but the key stakeholders, looks and feels very real—and that will probably deliver some sobering lessons.

Conclusion

The first step in managing the cyber risk associated with sensitive data is to adopt the mindset that cybersecurity isn't an IT problem to solve—it's a business risk to manage.

Cybersecurity needs to be a board-level issue, alongside concerns like business growth, continuity planning and governance, with regular metrics and reporting showing progress toward business outcomes. It should also be regarded as a proactive investment in risk management and harm reduction, rather than a cost.

It's also worth noting that compliance does not equal protection: that is, meeting the standards of HIPAA, PIPEDA, PCI, and other regulatory frameworks is related to—but very much separate from—creating a strong security posture.

By uncovering gaps, weaknesses, and blind spots, proactive risk management programs highlight shortcomings that attackers can exploit and allow you to direct finite security resources to effectively minimize business risk over time. Once you recognize the reality of cyber threats, your organization can extend beyond the fundamentals of a layered defense and adopt a risk-based approach to cybersecurity that includes:

- ✓ **Phishing and Security Awareness Training** to build a culture of cyber resilience.
- ✓ **Vulnerability management** to uncover exposed assets and direct patching efforts.
- ✓ **Penetration testing** to assess the organization's ability to detect and repel attacks.
- ✓ **Red team engagements** to replicate a real-world attack as closely as possible.

These services are not substitutes for protection of endpoints, networks, and cloud environments. Rather, they are necessary augmentations that help organizations to get the most out of their technology investments while reducing operational burdens.

Additionally, there's no better way to test your defenses than actually testing your defenses—that's why penetration testing and red teaming are so essential.

Just like you how you should test your backups and your restoration process, rather than simply trusting that everything will work, you should test your ability to detect and respond to intrusions into your IT environment that threaten your sensitive data.

Test, assess, and measure your cyber resilience

eSentire Managed Risk Services measure your current security posture through a framework of industry best practices and regulatory compliance requirements.

Our risk management team helps you identify blind spots, build a strategy for mitigating risk and operationalizes capabilities to predict and prevent known threats. Our managed risk program works hand in hand with our multi-signal Managed Detection and Response (MDR) and Incident Response services to deliver high fidelity detection and complete response.

We support in assessing, testing, and refining your strategic security plan.

The results? Your security program becomes adaptable to business performance drivers and the evolving threat landscape. Your defenses are hardened, risks are managed, and you can take control of cyber risk.

Our Difference	**Identify Potential Blind Spots**	**Build a Defensive Strategy Against Associated Risks**	**Operationalize Mitigation Capabilities**	**Measure and Adapt to Objectives and Threat Landscape**
Your Results	Alleviates resource constraints in your organization	An enterprise-level information security program with strong policies and procedures	Meet and exceed compliance requirements	Align business objectives with your unique risk and exposure

Ready to get started?

Connect with an eSentire Security Specialist to learn more about how you can reclaim the advantage and put your business ahead of disruption with eSentire's Managed Risk Programs.

Contact Us

If you're experiencing a security incident or breach contact us ☎ 1-866-579-2200

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.