eSENTIRE

The Vulnerable Landscape:

Metrics, Insight and Impact for Security Leaders

Executive Summary

When it comes to cyber resilience, the stakes have never been higher for modern companies. In the past two years, fourty-eight percent of businesses have suffered a data breach.[1] As cybercriminals get faster, more organized and increasingly ambitious, cybersecurity professionals must be vigilant to keep them at bay. This means shutting down vulnerabilities by patching assets as quickly as possible.

For most companies, it is not easy to stay ahead of the bad guys. Increasingly complex IT infrastructures make it difficult to find flaws and gaps that naturally increase with the sprawl. seventy-three percent of organizations say risk management is more difficult than it was two years ago, with increasing cloud workloads and software vulnerabilities cited as reasons for this sentiment.[2]

While identifying vulnerabilities is one part of the equation, continuous tracking, prioritization and patching proves the more daunting task that many companies do not have the staff to support. In fact, sixty-four percent of organizations want to add headcount to deal with this issue, but this alone is not enough. As vulnerability volume increases, the appropriate technology and processes associated creates a multifaceted problem for which headcount alone cannot correct.

As a result, security leaders find themselves without the appropriate resources to effectively address the riskiest vulnerabilities before attackers find and exploit them. In fact, fifty-seven percent of data breach victims were compromised via a vulnerability for which a patch was available. While the cyclical process of cat and mouse will continue, security teams can rebalance the equation with the appropriate approach to vulnerability management taking into account key topics covered in this report:

In this report you will learn:

- Exploiting vulnerabilities from the mind of an attacker
- Observed success and probability of an incident due to exploitation
- The metrics to help you prioritize vulnerabilities
- How to compliment your existing approach
- How eSentire services such as Managed Vulnerability Service and Managed Detection and Response can help

[1] Ponemon Institute, “Today’s State of Vulnerability Response: Patch Work Demands Attention”
[2] ESG/Tenable “What’s the Answer to the Vulnerability Overload Problem?”

Inside the mind of a hacker

To properly defend, one must understand what they are defending against. In an unfortunate imbalance, the comprehensive process of vulnerability management is much greater in scope than the approach an attacker needs to take to achieve their goals. While an attacker must find one point-in-time weakness, organizations must account for all vulnerabilities and prioritize mitigation on an ongoing basis. Consequently, understanding an attacker's mindset is critical to greater efficiency in defensive approach.

7.3 DAYS the average head start attackers have on security teams.

(Quantifying the Attacker's First-Mover Advantage, Tenable 2018)

A successful attack has several stages:

RECONNAISSANCE

This is where an attacker gathers information to profile a target in advance of an assault. They will use technical tools including network enumeration to find IP addresses and understand what devices and software versions they host.

Attackers complement these scans with open source intelligence to find useful information about a victim in the public domain. Technology job postings can show what products a company uses. Social media, news articles, technical reports and internal documents left exposed on web sites help to create organizational charts and identify key personnel to hit with social engineering attacks.

EXPLOIT MAPPING

Armed with a detailed infrastructure map, the attacker can then look for vulnerabilities in the target's hardware and software, along with associated exploits. They can find these in places including dark web forums, public databases such as Exploit-DB.com, CVE lists from NIST and MITRE, and penetration testing tools like Metasploit. By the end of this step, they will have a prioritized list of weapons to apply in the next step.

EXPLOITATION

The attacker launches their exploits. Delivery channels range from malware delivery via email (phishing) to malicious web application input.

These attacks do not have to be technically sophisticated. They could use human weaknesses to cajole or trick an employee into helping them. The hacker might pretend to be from the IT department and persuade a victim to install TeamViewer for remote access, for example. Or they could exploit weak or reused passwords.

PERSISTENCE

Most modern attackers want to remain undetected in the target's system. They will find a foothold in the target infrastructure from which they can spread laterally and build a persistent presence. Smart hackers live off the land using legitimate tools to infect more machines rather than malicious ones. This helps to avoid detection.

EXECUTION

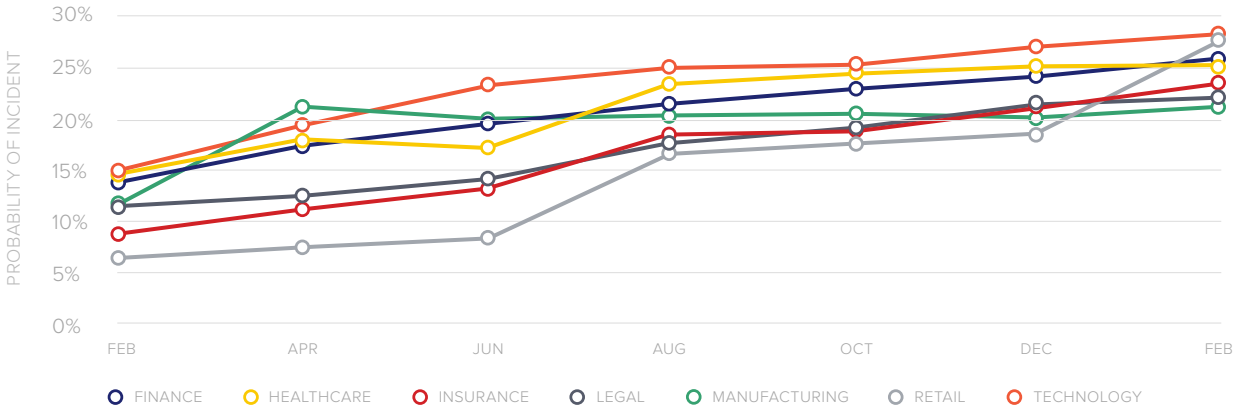
Once firmly established in the infrastructure, the attacker can achieve their goal, which is often exfiltration. They will transmit data from the client's system as quietly as possible.

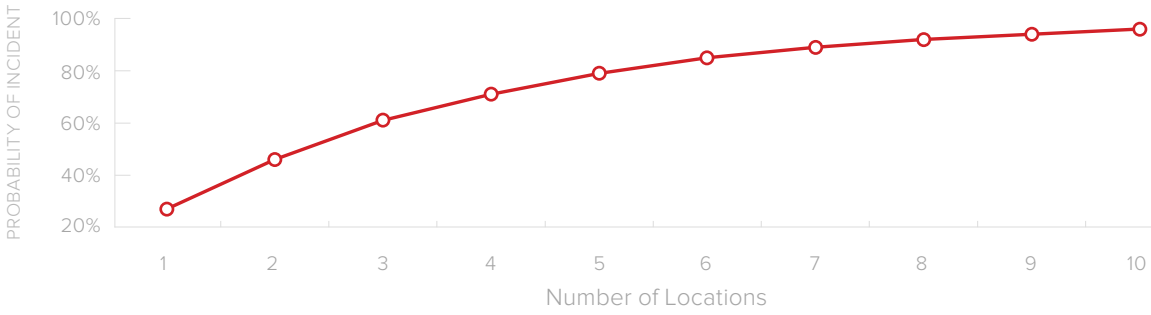
Observed Success of Attackers

An attacker using these techniques need only be successful once. Unfortunately, observed rates of success indicate adversaries will eventually find an unaccounted for blind spot given a long enough timeline.

Based on a recent study from eSentire's SOC, leveraging data from over 1,600 network sensors and 87,000 endpoints, we were able to predict the probability of an incident (in this case due to an exploit) that bypassed existing controls.

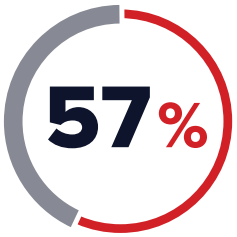
We found that the cumulative probability of an exploit incident increased steadily over time for all industries. Technology topped out with a thirty-one percent chance that an incident would occur at the end of a 12-month period, with the global average at twenty-six percent. These trends reflect single site locations. Unsurprisingly, the more locations in an environment the more the risk of exploitation compounds. For clients between five and ten locations, the risk of exploitation ranges from seventy-nine to ninety-six percent.





Important Vulnerability Metrics for Security Leaders

While the probability models paint an alarming picture, the intent is not to portray impending doom. Many of the organizations represented in the data are underresourced to adequately account for the environmental sprawl and ocean of data that must be interpreted and actioned to effectively identify and prioritize vulnerabilities. With vulnerability management being a marathon rather than a sprint, it is important to look at certain metrics that are key indicators of potential risk and proof of continuous hardening of defenses against exploitation.



of organizations claim they lack a formalized vulnerability tracking process.

— Ponemon Institute, "Today's State of Vulnerability Response: Patch Work Demands Attention"

CRITICALITY

Bugs have different severity levels including critical (e. g., remote code execution), high, medium, low and informational. These can help you prioritize which to address first.

AFFECTED ASSETS

Some bugs will not touch any software or equipment in your organization, while some only affect low-risk assets. A vulnerability's priority will increase along with the risk profile of its asset.

EXPLOITS IN THE WILD

Just because a bug has not been visibly exploited does not mean that it is safe. The recent zero-day WinRAR discovery is a perfect example of this. The vulnerability itself dates back to the early 2000s, but the exploit itself became known to the information security community in 2019.[3]

RECURRENCE

Are you seeing the same vulnerabilities regularly cropping up in your environment? If so, it is worth looking at systemic changes to address them.

AVERAGE VULNERABILITY AGE

This metric demonstrates progress or the lack of it. If it remains high, you are treading water. If it decreases, you are gaining ground.

SECTOR-WEIGHTED PERFORMANCE

eSentire's Security Operations Center (SOC) data can show your incidents of compromise vs your industry so that you can measure your remediation efforts against your peers.

[3]https://threatpost.com/winrar-flaw-500-million-users/142080/?_ga=2.71739094.490281215.1556549708-959256911.1548274696

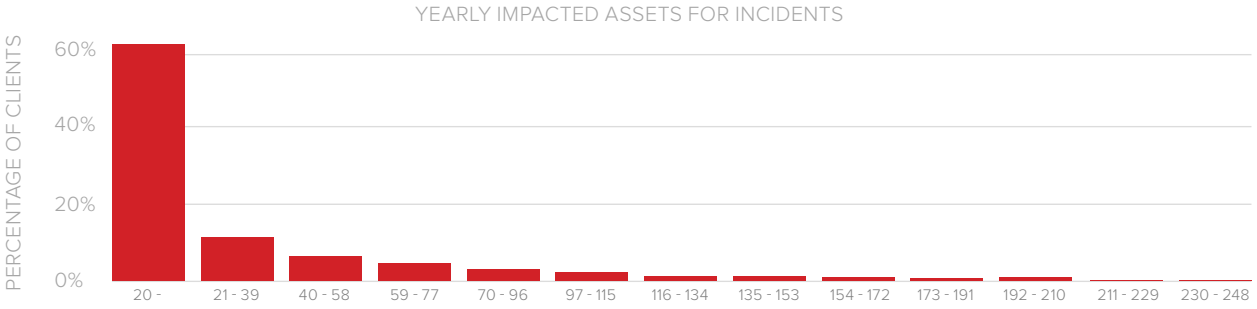
Complimenting Your Vulnerability Management Approach

Vulnerability management is a continuous and resource-intensive process. While many organizations attempt to identify, prioritize and remediate vulnerabilities on their own, the majority of organizations find the investment too great for already underresourced security teams.

In recent studies, organizations on average are dedicating 321 hours a week to managing vulnerability response, representing twenty-nine percent of all security personnel time. Sixty-four percent of these organizations anticipate the need for increased headcount dedicated to vulnerability management with fifty percent of them already in their planning stages.[4]

At eSentire, we look to compliment your existing approach with a mixture of detailed metrics and insightful appraisal from experts who understand cyber risk and the mindset of adversaries. Our latest offering, Managed Vulnerability Service, is a co-managed vulnerability management platform that delivers powerful vulnerability analytics leveraging industry-leading technology in combination with dedicated human experts who act as an extension of your team. In addition, our Managed Detection and Response acts as a last line of defense, detecting and responding to threats that circumvent existing security controls.

The graph below depicts eSentire Managed Detection and Response clients that had an incident due to an exploit bypassing existing security controls seventy-two percent were able to restrict affected assets to 39 or less over a 12-month period. Put more plainly, this means organizations of all industry type and size are challenged with vulnerability management and would have been at serious risk of a breach if it were not for eSentire's SOC analysts detecting the exploitation and taking action on the client's behalf. This certainly is not an indictment of our client base, but rather a confirmation of the industry-wide problems described in this report. Security leaders familiar with the complexity of managing vulnerabilities will likely find this data is unsurprising and further confirms the business need for a service such as Managed Vulnerability Service.



In conclusion, the impact is clear: if you are unable to prioritize and patch your assets, then the probability of successful intrusion will eventually near 100 percent. The earlier you can catch a vulnerability, the easier it is to stop a breach from happening in the first place. If you are unable to patch a vulnerability in time, then additional layers of defense that include timely detection and response capabilities are critical.

The key is the effective combination of human expertise, refined processes and reliable technology. Combining eSentire Managed Vulnerability Service and Managed Detection and Response gives organizations the peace of mind necessary to grow the business while mitigating risk with confidence that time and investments are where they can be most effective.

[4]Ponemon Institute, "Today's State of Vulnerability Response: Patch Work Demands Attention"

eSentire, the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyber attacks 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.**