Balbix®

Ponemon INSTITUTE

February 2019

Challenging State of Vulnerability Management Today:

Gaps in Resources, Risk and Visibility Weaken Cybersecurity Posture

In the last two years, businesses and governments have seen data breaches like Equifax and Marriott impact 100s of millions of accounts each, as well as critical intellectual property (IP) and core operations. A global survey of 600+ cybersecurity leaders and professionals by Ponemon Institute shows that 67% of organizations are not confident that they can avoid a data breach, and what the primary security and IT challenges that are causing this. The survey also provides fundamental recommendations that can reduce breach risk through innovating and improving a vulnerability management program.

Table of Contents

Executive Summary

Too many organizations are struggling to maintain or improve their security posture, as exemplified by their lack of confidence in avoiding a breach and inability keep up with even basic patching and vulnerability management. In a recent research project, Ponemon Institute found that only 1 in 3 organizations are confident that they can avoid a data breach, and that 63% are unable to act on the large number of alerts and actions generated by their vulnerability management program.

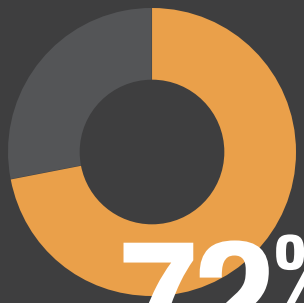
Some of the common challenges that organizations face include not enough staff to cover the volume of alerts, vulnerability management solutions that complicate the ability to patch in a timely manner, not enough visibility across their full set of assets and attack vectors, and a lack of understanding of actual cyber-risk and inability to prioritize mitigating actions. The goal of this research was to better understand the barriers to an effective vulnerability and risk management program and how they can be overcome.

The Challenging State of Vulnerability Management was sponsored by Balbix and performed by Ponemon Institute, which surveyed 613 IT and IT security leaders and professionals who are involved with vulnerability management within their organizations. To provide a path towards a stronger cybersecurity posture, the study investigated the characteristics and requirements of both mainstream and high-performing security organizations that have and operate vulnerability management programs.

Providing insights into both core challenges and major gaps that mid-size to large organizations are seeing today – as well as recommendations for best practices and new capabilities to explore – this report presents tangible guidance for improving vulnerability management programs and better avoiding data breaches. Recommendations include discovering your full attack surface, understanding your cyber-risk and the risk of each asset if it were breached, using cyber-risk to prioritize what gets fixed (to offset the massive volume of incoming alerts), and making SecOps more productive by automating all these activities and creating tickets to get them executed.

600
cybersecurity professionals

15+
vertical industries

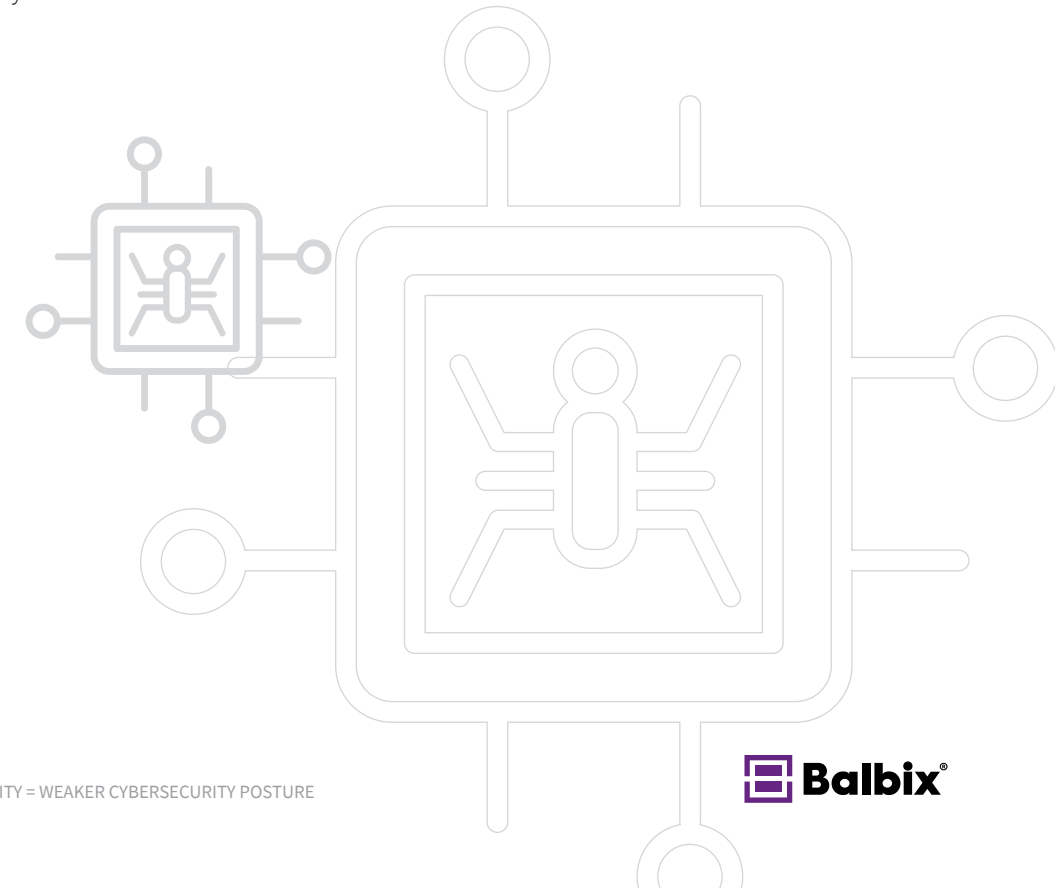


72%
of respondents worked at companies with more than 1,000 employees

Methodology

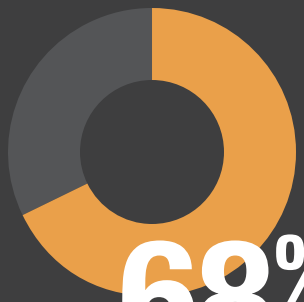
Balbix commissioned the Ponemon Institute to survey over 600 cybersecurity professionals across 15+ vertical industries. 72% of respondents worked at companies with more than 1,000 employees.

Founded in 2002, the Ponemon Institute is a research center specializing in data protection and information security policy.



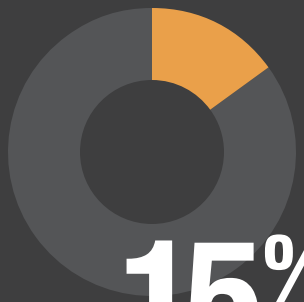
Balbix®

Per survey respondents, security teams' key challenges with vulnerability management include:



68%

feel that staffing is not adequate for a strong cybersecurity posture



15%

say their patching efforts are highly effective

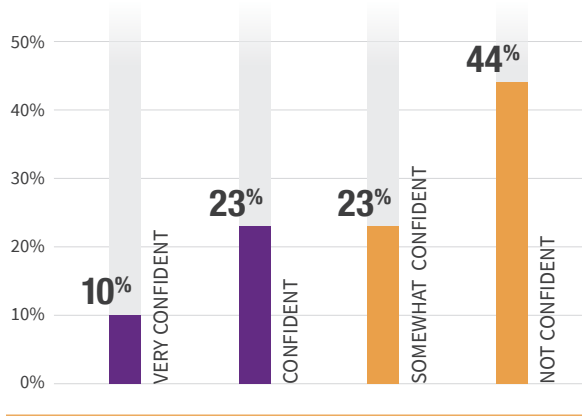
Maintaining Security Posture is Hard…Vulnerabilities Make it Harder

Too many organizations are struggling to maintain or improve their security posture. The attack surface of a modern enterprise is massive. A typical enterprise has a bewildering variety of assets: infrastructure, applications, managed and unmanaged endpoints (fixed and mobile), IoT and cloud services. There are practically unlimited permutations and combinations in which things can go wrong. Users can be phished. Weak passwords, software vulnerabilities, misconfigurations and numerous other vectors can be leveraged to compromise some internet-facing enterprise asset and gain an initial foothold inside your network. Once in, the adversary can usually move across the enterprise rapidly to locate and compromise some important asset — and you have a major breach.

This complexity is clearly exemplified in security leaders' lack of confidence in avoiding a data breach.

As shown in Figure 1, only 10 percent of the 600+ survey respondents are very confident that they can avoid a data breach and maintain a strong security posture.

Figure 1. How confident are you that your organization can avoid a data breach?



One good example of the difficulty in maintaining (or improving) one's security posture is the challenge to keep up with even basic software vulnerability management and patching – a fundamental but key component of security posture.

Balbix®

SecOps Resources Can't Keep Up with Volume of Vulnerabilities

A key research finding is that security teams cannot properly resource the management of vulnerabilities – both identifying and patching – to confidently avoid a data breach. While this complaint is common throughout most practices within cybersecurity teams, and IT organizations in general, it has become acute in vulnerability management because of the sheer volume of alerts for unpatched systems.

67%

feel they do not have the time and resources to mitigate all vulnerabilities in order to avoid a data breach

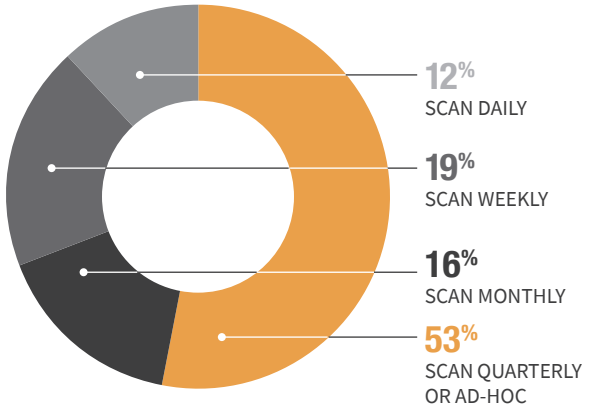
This challenge has gotten continually harder month-over-month and year-over-year due to the number of systems and applications being regularly added for business growth as well as the ongoing digitization of business processes. Thus, patching is taking an increasing amount of the security and IT teams' time budget every month.

To make things [much] harder, vulnerability management solutions have not evolved to counter the growing number of alerts generated with each scan, and don't have the technology to help teams prioritize which patches to address immediately and which to postpone – resulting in a "roulette-like" approach to picking which patches to address.

63%

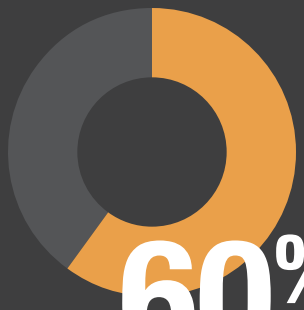
of respondents with ineffective vulnerability programs (59% of total) say "inability to act on the large number of resulting alerts and actions" is problematic

Even with this significant percent of time pool committed, and the noted 63% inability to act on open alerts, security teams are not running their vulnerability management scans frequently enough! Ponemon survey research finds that only 31% of respondents are scanning more than once a month, half are only scanning quarterly or have no formal schedule at all, and less than half use up-to-date software patching to avoid data breaches.



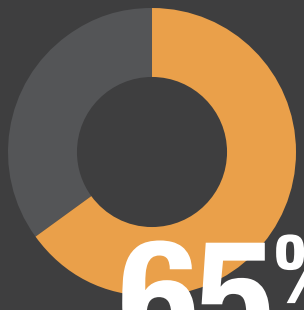
Just over two-thirds of all respondents admit being quite behind (once a month or less frequently) on fixing known software vulnerabilities. And less than half consider up-to-date patching as a proactive approach to avoiding breaches.

These statistics are telling, as this type of attack vector is often the easiest way for an adversary to get in, as sample exploit code for such attacks is widely available for anyone to download and weaponize. What this means is that in enterprises operating this way, an Equifax-like breach is just one bad click away.



60%

report not enough visibility across all IT asset types (especially unmanaged assets) as a big challenge



65%

want vulnerability management tools to automatically discover unmanaged assets

Many IT Components of the Business Aren't Covered

While alert volumes and limited SecOps staff resources are a major challenge to operating a successful vulnerability management (VM) function, another key issue is visibility across the full range of an organization's vulnerable IT assets.

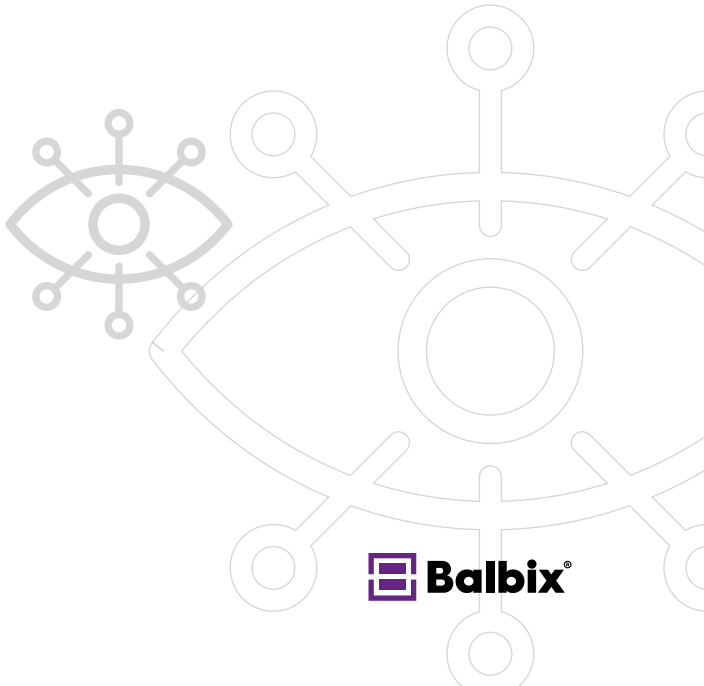
Traditional VM tools scan a fairly limited set of assets – usually corporate-owned or managed IT infrastructure (servers, storage, network), internally hosted applications, and endpoints (notebooks/ desktops). While most VM tools support public cloud-based instances of infrastructure and hosted apps, there is a large percent of corporate IT assets that are not seen, analyzed or reported on:

- Bring your own devices (BYOD) such as mobile phones, tablets and increasingly notebooks
- IoT assets
- Industrial equipment (ICS)
- Transient assets
- Assets used by third-parties (e.g. resellers, supply chain partners, consultants, etc.)

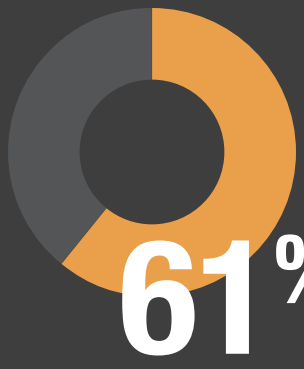
Surprisingly, many VM tools don't even discover or scan unmanaged assets.

Additionally, the scope of scans with most VM tools has to be set up manually by security teams, often consulting out-of-date inventory databases of static IP addresses and dynamic IP ranges.

The net result is that current VM tools have not kept pace in bringing automatic discovery, visibility and vulnerability assessment to the growing spectrum of IT components in today's business strategy – thus impeding vulnerability management programs' ability to ensure their organizations' security posture and cyber-resilience.

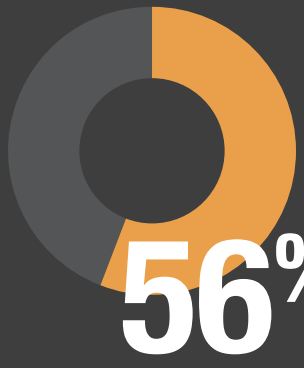


Balbix®



61%

say they don't have adequate context on the business impact if a vulnerable asset got breached



56%

are concerned about their inability to predict where or which assets would be compromised

Can't Get Cyber- (or Business) Risk for IT Assets

Another subtler, but very fundamental, challenge that survey respondents note is their lack of understanding of the cyber- and business risk of each of the tens or hundreds of thousands of IT assets that access their network.

As noted earlier, the current level of alerts created by vulnerability management tools and scans in not achievable by the majority of security and IT ops teams. With additional context information beyond general vulnerability ratings like CVSS scores, SecOps teams would be able to much more efficiently and effectively address the most critical vulnerabilities found on their wide portfolio of IT assets.

The most important information is about the actual risk of an asset if it were breached – both cyber-risk and business risk. Core to understanding both types of risk is context – i.e. "what is the role of the asset", "what data does it use or store", "what else is it connected to", etc. Current VM tools do not provide context for any or all of the thousands of assets they regularly scan and create alerts for.

As a result, the majority of security teams don't incorporate risk into their vulnerability management activities, and don't get either the increased resiliency/better security posture or a manageable scope of work.

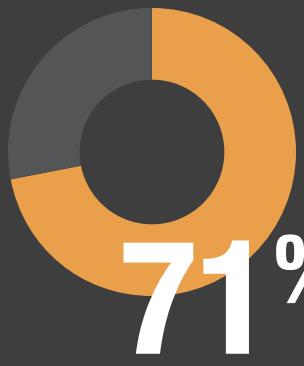
Only 40% of organizations even attempt to incorporate business risk into its vulnerability management activities

Another result of this lack of context and ability to establish the risk level of each IT asset is the inability to predict what assets are most likely to be breached, which is a key concern for both SecOps teams and CISOs alike.

Without appropriate business context and understanding of business risk, security teams can spend their scarce vulnerability management resources on software vulnerabilities that have low risk while leaving critical vulnerabilities (which carry great risk) open for long period of times, providing wide-open doors for their adversaries to use. This painful lack of risk understanding and vulnerability prioritization is a major reason behind the poor security posture of many organizations.

39%

say their leaders recognize the criticality of effective vulnerability management in avoiding data breaches



71%

feel that their executives and senior management do not communicate their risk goals clearly to security team

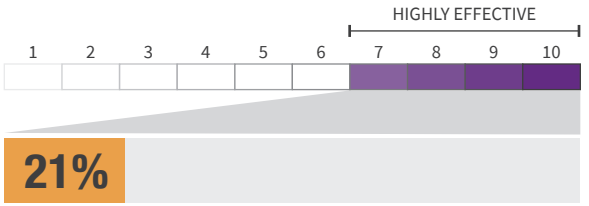
Communications Silo with C-suite on Cyber-risk

Only 9% feel that security teams are highly effective in communicating security risks to C-suite and boards

C-suite and IT security functions operate in a communications silo. Communication and collaboration between senior management and the IT security leadership is affected by the fact that the majority of organizations have senior leaders that don't recognize or understand how vulnerable they are, and the importance of vulnerability management. Only 39 percent of respondents say their organizations' leaders recognize that effective vulnerability management is critical to avoiding a data breach or other security incident.

Both the C-suite and the IT security function are not effective in jointly communicating risk management priorities and cybersecurity threats. Only 29 percent of respondents say their organization's executives and senior management clearly communicate their business risk management priorities to the IT security leadership.

Additionally, IT security teams are often not effective at communicating cybersecurity risks to senior management. On a scale of 1 = not effective to 10 = highly effective, only 21 percent of respondents (7+ on the 10-point scale) say their communications are highly effective.



Only 21% of respondents say their communications are highly effective

Those that are effective cite the best way to communicate cybersecurity risks is to make technical information understandable, up-to-date and helpful in making decisions.

65%

We present technical information in a way that is understandable

63%

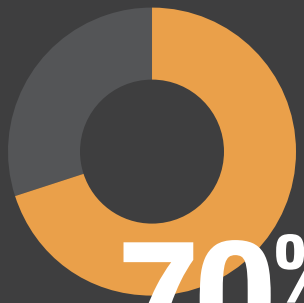
We keep our leaders up-to-date on cybersecurity risks and don't wait until the organization has had a data breach or security incident

63%

The information we present is not ambiguous and is helpful to making decisions

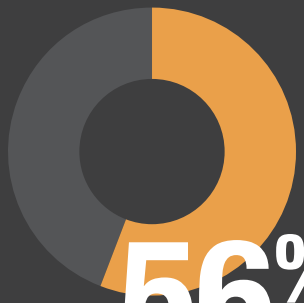
Balbix®

What capabilities would most improve your vulnerability management program:



70%

want to automatically discover unmanaged assets



56%

want to receive a risk-based and prioritized list of actions

No Easy Answers, But Some Good Ones

As this research has shown, maintaining and improving your security posture is a very challenging initiative, and the current state of most vulnerability management and patching programs makes it that much more difficult.

Respondents – especially those rated as "high performing organizations" – understand the vulnerability management challenges cited in this research and what incremental capabilities could best answer them. When asked what would most improve their vulnerability management program and tools, high performing responders cited the ability to:

64%

analyze vulnerabilities in IoT, BYOD and third-party systems

60%

analyze both unpatched systems and other attack vectors

52%

receive prescriptive fixes per recommended action

Balbix®

Recommendations

Now it's your turn. The volume of data breaches is already extremely high and will only grow further in size, frequency and impact. Organizations can't continue to rely on the legacy vulnerability management systems, scope of analysis and manual processes they have in place today. Security, SecOps and vulnerability teams can learn from organizations that effectively avoid breaches and start adding new capabilities and processes to address the challenges widely called out in this research.

Here are four fundamental recommendations for your vulnerability management program to better avoid a data breach and transform your company's security posture:

1 Fully discover your attack surface – everything that touches your network, and every way it might get attacked

Make it a goal to automatically discover all internal, cloud and third-party IT assets that touch your network and could be an entry point to your organization. This is a much broader set than just your servers, applications, managed IT infrastructure and cloud assets – it also includes BYOD (mobile, notebook), IoT assets, industrial control systems (ICS) and very importantly, third-party assets from supply chain/reseller/alliance and other business partners. Any asset from any of these asset classes could be one click or connection away from starting a major data breach if not discovered/analyzed/monitored continuously.

Just as important as seeing all your connected assets is monitoring them across all potential attack vectors (250 and counting, including phishing, malware, password hygiene/sharing/non-encrypted, etc.). Traditional vulnerability management focuses primarily on one key, but only one, attack vector – unpatched systems, leaving attackers with many other ways to penetrate your network and execute a breach.

2 Understand your overall cyber-risk and the specific business risk of each asset if it were breached

As noted in the Ponemon research, the majority of organizations (60%) haven't incorporated cyber-risk into their vulnerability management program. By adding the capability to assess the cyber-risk of every asset touching your network – and their interaction with users and each other – you can extrapolate and determine the total cyber-risk of your enterprise, as well as assess and improve your cybersecurity posture.

3 Use risk-based analysis to prioritize which fixes SecOps and IT teams should work on, postpone and ignore

Also noted in the Ponemon research is a major gap between incoming alerts and SecOps/IT team resources to work through them. 63% of respondents cite their "inability to act on the large number of alerts and actions" coming from their vulnerability management systems.

By understanding your device- and organization-level cyber-risk (as noted above), you can use risk to prioritize the huge, growing set of alerts provided by your vulnerability management system. The output of that process should be a clear and prioritized list of what issues to fix in what order (e.g. unpatched software, password issues, misconfigurations, etc.), ideally with instructions on how to fix them. This is much more granular and guided than simply being told after a vulnerability scan (or penetration test) to "patch 1000s of servers due to a recent vulnerability or new threat discovery". Rather, this is a clear set of guidance on what actions to take to minimize breach risk, regardless of how many resources are on your team, because they are prioritized asset-by-asset based on business risk.

4 Make SecOps and IT more productive by automating the discovery of asset inventory and vulnerabilities, as well as the creation of prioritized fixes and resulting tickets

Automation is viewed as one of the key technical objectives of current cybersecurity programs, and has created new market categories like security orchestration, automation and response (SOAR). Wrt improving vulnerability management programs, each of the processes noted above can be achieved only if it is automated. This is due to the immense volume of data to be analyzed to deliver the resulting information, be it discovery and status of tens of 1000s of assets or comparative risk assessment of all your assets to produce a prioritized list of actions. Automation of ticket creation and integration into existing workflows is also required to achieve the needed volume of mitigation actions.

When assessing new tools and technologies to achieve this level of automation, carefully assess how they do or don't utilize AI and machine learning to enable the level of processing required. Putting aside that marketing and "AI-washing", understand how the tool is able to automatically find and examine the data needed to actually automate a process and deliver the tangible outcome noted in the recommendations above.

Balbix

3031 Tisch Way, Ste. 800
San Jose, CA 95128
866.936.3180

info@balbix.com
www.balbix.com