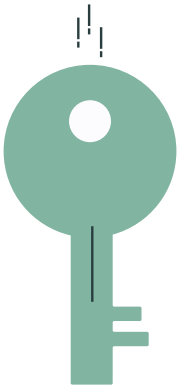
servicenow | Ponemon INSTITUTE

THE STATE OF VULNERABILITY RESPONSE IN HEALTHCARE:

PATCH WORK DEMANDS ATTENTION

In the last two years, 50% of healthcare organizations have experienced a data breach, and the severity and volume of cyberattacks continue to increase. A global survey of 322 cybersecurity professionals shows that healthcare firms can dramatically reduce the risk of being breached by improving end-to-end vulnerability response processes.

EXECUTIVE SUMMARY



Major data breaches attract widespread media coverage and intense public scrutiny. For organizations that suffer a breach, the consequences can be catastrophic, ranging from loss of brand reputation and consumer confidence through to economic impacts that severely damage the bottom line. As hackers ramp up their attacks and turn to advanced technologies such as artificial intelligence, it is essential that cybersecurity teams keep pace, fending off attacks and keeping sensitive data secure.

However, widely publicized data breaches are only the tip of the iceberg. ServiceNow surveyed 322 cybersecurity professionals at healthcare firms around the globe, and found that almost half of these organizations suffered a data breach in the last two years. Of these, the majority said that they had been breached because of a vulnerability—for which a patch was already available. This highlights an overwhelming need for more effective vulnerability response, closing down these attack vectors before hackers strike.

To shine a light on the way forward, the study investigated the characteristics of organizations that avoided breaches. These organizations consistently rate their abilities higher in two key areas: detecting vulnerabilities and patching vulnerabilities in a timely manner. Of these, timely patching was the most significant factor.

However, many healthcare firms face the "patching paradox"—hiring more people does not equal better security. While security teams plan to hire more staffing resources for vulnerability response—and may need to do so—they won't improve their security posture if they don't fix broken patching processes. The study shows that firms struggle with patching because they use manual processes and can't prioritize what needs to be patched first. Coordinating vulnerability response across multiple teams exacerbates this struggle, leading to long delays and vulnerabilities that slip through the cracks.

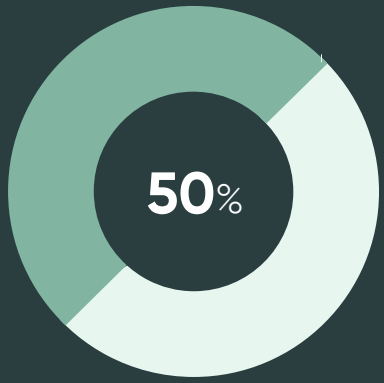
Armed with these insights, this report presents a pragmatic roadmap for reducing data breaches. These recommendations include paying attention to basic hygiene items, breaking down silos between tools, creating structured workflows for vulnerability response processes, and automating these workflows as much as possible. By following these recommendations, healthcare organizations can emulate the success of today's cybersecurity leaders, dramatically reducing risk for their business and their customers.

METHODOLOGY

ServiceNow commissioned the Ponemon Institute to survey nearly 3,000 cybersecurity professionals. Of those surveyed, 322 were from healthcare organizations. Respondents were based in Australia, France, Germany, Japan, the Netherlands, New Zealand, Singapore, the United Kingdom, and the United States, and represented companies with more than 1,000 employees. The survey was administered online.

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

HALF OF HEALTHCARE ORGANIZATIONS HAVE HAD A RECENT DATA BREACH



50% of respondents reported one or more data breaches in the last two years

Major data breaches are headline news. When a healthcare provider or payer exposes patient data to hackers, the public outcry is immense. Whenever cybercriminals steal confidential Protected Health Information (PHI), it is a public relations nightmare with long-lasting consequences.

The costs are staggering. According to a 2017 Ponemon study, a breach involving as little as 10,000 records costs the breached party an average of $2.8 million. Overall, the cost is $141 for every record lost, and this rises to more than $380 for healthcare organizations in the United States. Scale this to a breach affecting millions of records, and the bottom-line economic impact is enormous.

However, well-publicized breaches are only the tip of the iceberg. Among 322 cybersecurity professionals at healthcare organizations surveyed by ServiceNow, half (50%) reported a data breach in the last two years.

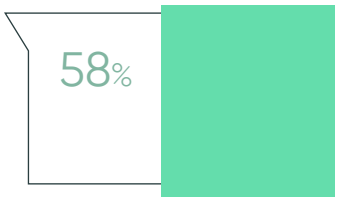
HACKERS ARE OUTPACING SECURITY TEAMS

15%

15% increase in cyberattack volumes over the last 12 months

22%

22% increase in cyberattack severity over the last 12 months



58% say attackers are outpacing enterprises with technology such as machine learning and artificial intelligence

These breach rates are likely to rise unless security teams adopt new approaches. The majority of survey respondents (58%) agreed that attackers are outpacing healthcare firms with technology such as machine learning and artificial intelligence (AI). Given the enormous potential for weaponized AI to transform hacking—everything from self-learning hivenets to radically more effective spear phishing—this is a significant source of concern.

This qualitative result is supported by data. Survey respondents reported an average 15% increase in cyberattack volumes over the last 12 months, and they said that the severity of these attacks increased by 22% over the same period.

Given this high and potentially growing breach rate, we wanted to know how high-performing healthcare security teams prevent breaches and what other teams can do to emulate their success.

CHARACTERISTICS OF HIGH-PERFORMING SECURITY ORGANIZATIONS AT HEALTHCARE FIRMS

The survey investigated how organizational capabilities affect breach rates. Respondents were asked to rate their organization's ability on a scale of one to 10 in several key areas. They were divided into two groups: those that had been breached in the last two years and those that hadn't.

Two key capabilities stood out for healthcare firms that avoided breaches. On average, they rated themselves more highly on:

- The ability to detect vulnerabilities quickly (6.90 vs. 5.95, or 16% higher)
- The ability to patch vulnerabilities in a timely manner (6.59 vs. 4.69, or 41% higher)

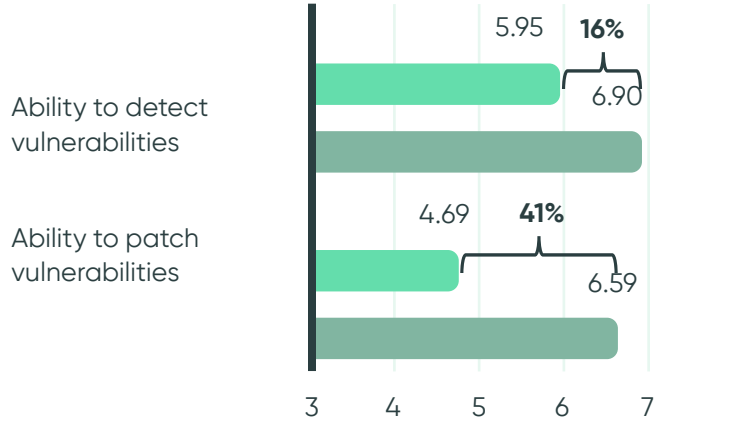
Healthcare firms that avoided breaches rated their ability to patch vulnerabilities in a timely manner 41% higher than those that had been breached, and they rated their ability to detect vulnerabilities 16% higher.

Patching is the most significant characteristic of firms that were not breached in the last two years.

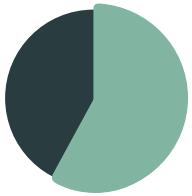
It isn't surprising that detecting vulnerabilities and patching vulnerabilities are key leadership characteristics. When a vulnerability is made public and a patch is released, the race is on. If a hacker can successfully attack before the target patches the vulnerability, there is a high risk of a data breach. And, hackers appear to be winning the race. Fully 58% of respondents who reported a breach said that they were breached due to a vulnerability for which a patch was available but not applied. 37% say they actually knew they were vulnerable before the breach occurred.

Given the importance of detecting and patching vulnerabilities, the study investigated how to close these two gaps, helping organizations avoid breaches.

CAPABILITY GAP



Respondents rate their ability in each area on a scale of 1 to 10



58%

of healthcare firms that were breached said they were breached due to an unpatched known vulnerability

37%

of healthcare fims that were breached knew they were vulnerable before they were breached

MANUAL PROCESSES AND SILOED TOOLS DELAY PATCHING

As noted previously, attack severity and volumes are increasing. However, hackers aren't just attacking harder and more often—they are also attacking faster. 48% of respondents from healthcare organizations said that the time window for patching—the time between patch release and hacker attack—has decreased an average of 28% over the last two years. As AI-fueled attacks become more prevalent, we expect that window to shrink even further.

To prevent data breaches, security teams need to patch more quickly. However, the survey shows that they are being held back by manual processes and disconnected systems that compromise their ability to patch in a timely manner. The majority of respondents from healthcare organizations (58%) say that they spend more time navigating manual processes than responding to vulnerabilities, and 52% agree that manual processes put them at a disadvantage.

28%

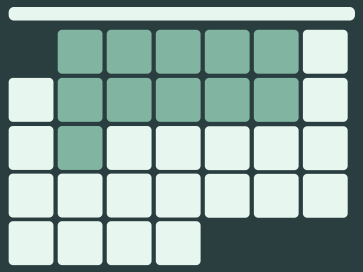
decrease in time window for patching before being attacked, over the last two years

52%

say that manual processes put them at a disadvantage when patching vulnerabilities

65%
say that it is difficult to prioritize what needs to be patched first

11 DAYS
lost coordinating activities across teams for every vulnerability patched



Coordinating across teams increases the patching challenge. Only 18% of respondents say their team is solely responsible for patching, while the rest report an average of 11.4 days lost coordinating across teams for every vulnerability they patch. Reasons for this include:

- Having no common view of assets and applications across security and IT (63%)
- Things slip through the cracks because emails and spreadsheets are used to manage the patching process (63%)
- There is no easy way to track whether vulnerabilities are being patched in a timely manner (76%)

And, it's not just about working slowly. 65% of respondents from healthcare organizations also say they find it difficult to prioritize what needs to be patched first. Again, this is a symptom of manual processes and disconnected systems.

To accurately prioritize vulnerabilities, you need to know both the severity—as measured by Common Vulnerability Scoring System (CVVS) scores, for example—and the types of business systems affected. However, these two pieces of information typically sit on opposite sides of the security/IT boundary. As evidence of this disconnect, only 26% of respondents said that they use both severity and types of business systems affected to prioritize vulnerabilities.

Security teams shouldn't be discouraged by the problems identified. Instead, these issues point the way forward to a stronger security stance. By automating routine activities and breaking down process and data barriers, security teams within healthcare organizations have the opportunity to dramatically accelerate the patching process—and to keep pace with external attackers.

THE PATCHING PARADOX:

HIRING MORE DOES NOT EQUAL BETTER SECURITY

43% headcount increase for patching in the next 12 months

This study uncovered the "patching paradox"—hiring more people does not equal better security. While security teams plan to hire more staffing resources for vulnerability response—and may need to do so—they won't improve their security posture if they don't fix broken patching processes first.

Cybersecurity teams in healthcare organizations already dedicate a significant proportion of their resources to patching. Respondents say that their companies spend 345 hours a week on average—or approximately nine full-time employees—managing the vulnerability response process. Since our survey showed that the average cybersecurity headcount is 22, this represents approximately 39% of security resources.

That number is set to rise. Because they are struggling with manual processes, 60% of respondents say that they plan to hire additional dedicated resources for vulnerability response over the next 12 months. Across these respondents, the planned headcount increase is 3.69 people. This represents 43% growth over today's staffing levels. Keep in mind that respondents came from organizations ranging from 1,000 employees to more than 75,000, so that headcount increase is likely to far exceed 3.69 in large healthcare organizations.

2 MILLION

global shortage
of cybersecurity
professionals by 2019*

However, healthcare organizations may not be able to hire their way out of vulnerability response shortfalls. According to ISACA, a global non-profit IT advocacy group, the global shortage of cybersecurity professionals will reach 2 million by 2019. The job site Indeed reports that demand far outstrips interest, with only 6.67 clicks for every 10 cybersecurity jobs posted in the US—meaning that at least one-third of postings get no views at all. That number drops as low as 3.50 clicks in Germany and 3.16 clicks in the UK. Against this backdrop, organizations will find it extremely difficult to secure the resources they need.

Given the process challenges facing security teams, additional staff will not solve the fundamental issue. As reported earlier, 63% of respondents say they have no common view of assets and applications between security and IT, 63% say that things slip between the cracks because emails and spreadsheets are used to manage the patching process, and 76% say there is no easy way to track whether vulnerabilities are being patched in a timely manner. All of these point to a lack of integrated, end-to-end processes that provide visibility and control across the entire vulnerability response lifecycle.

Automation offers a path forward. By automating routine vulnerability response processes and elevating staff to focus on more critical work, security teams can dramatically reduce breach rates while making the most of existing staff.

* Source: ISACA, 2016

RECOMMENDATIONS

The time to act is now. Breach rates are already extraordinarily high, and emerging AI-fueled threats are likely to increase the volume, speed, and effectiveness of cyberattacks even further. Healthcare organizations can't rely solely on hiring amidst a talent shortage to get work done with the manual processes they use today. Security teams need to learn from firms that avoid breaches and focus on resolving the issues identified in this report.

ServiceNow helps organizations resolve security incidents and vulnerabilities fast. Based on best practices developed with customers, here are five key recommendations from ServiceNow that provide organizations with a pragmatic roadmap to reduce the risk of a breach:

1 | Take an unbiased inventory of vulnerability response capabilities. Assess maturity based on the two key capabilities of healthcare organizations that avoided a breach: detecting vulnerabilities and patching them in a timely manner. Identify problematic areas, such as cross-department coordination, lack of asset and application visibility, and inability to track the vulnerability lifecycle. Score these areas by estimating the existing risk—for example, based on the delays they introduce into the vulnerability patching process.

2 | Accelerate time-to-benefit by tackling low-hanging fruit first. Start with basic hygiene items that can be addressed quickly. For instance, if security teams don't scan for vulnerabilities, they need to make it a top priority to acquire and deploy a vulnerability scanner. If they do scan, they need to make sure they are doing both external and internal scans, including authenticated scans. Prioritization of vulnerabilities is also essential—for example, based on scanner scores or CVVS scores as well as understanding the business importance of the affected system. By integrating threat intelligence, security teams can factor in whether a vulnerability has been weaponized or is part of an active campaign.

3 | Break down data barriers between security and IT. Create a common view combining vulnerability and IT configuration data—ideally using a single platform. This lays the foundation for more advanced capabilities, such as prioritizing vulnerabilities based on impacted business systems and routing vulnerabilities to the right IT system owners for patching.

4 | Define end-to-end vulnerability response processes, and then automate as much as possible. Repeatable vulnerability response processes increase accuracy—reducing risk and eliminating rework. Workflow and process automation adds to this by driving significant efficiencies, accelerating patching times and reducing staffing requirements. Pay attention to automated routing, status tracking, measurable SLAs, and automated escalations. Ensure that security teams and IT teams have a shared view of these processes, and create situational awareness by providing dashboards and heat maps.

5 | Retain talent by focusing on culture and environment. People want to work in high-performance organizations where success is the norm. Creating this environment is the best way to attract and retain talent, particularly when competition is high. By breaking down internal barriers, creating optimized processes, and automating mundane work, security teams can dramatically increase job satisfaction and eliminate frustration—making their firm a preferred place to work.

CONCLUSION

In a world where hackers are becoming faster and more intelligent, cybersecurity teams need to redouble their efforts to keep data secure. Given that the majority of victims are breached because of unpatched known software vulnerabilities, effective vulnerability response is a critical weapon in the cybersecurity arsenal. High-performing security teams consistently outperform because they detect vulnerabilities quickly and patch them in a timely manner. To emulate the success of these healthcare organizations, security teams need to create the same core competencies.

However, many cybersecurity teams are struggling to build these capabilities. They are disadvantaged by manual processes, wrestle with siloed tools and data, and don't have the resources they need to patch in a timely manner. As a result, these teams suffer significantly higher breach rates, putting their hospital systems, patients, and employees at risk.

The good news is that these barriers are not insurmountable, as high-performing security teams demonstrate. By automating routine processes and taking care of basic hygiene items, security teams can significantly reduce the risk of a breach. With a pragmatic roadmap, these results are within reach of any healthcare organization, offering hope for a more secure future.