DEMYSTIFYING VULNERABILITY MANAGEMENT

F-Secure®

TABLE OF CONTENTS

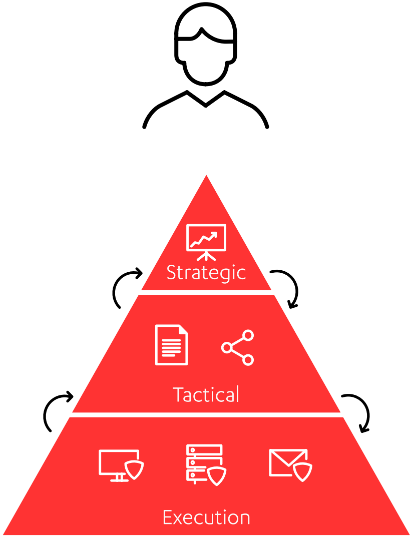
PART I: MITIGATING CYBER RISKS WITH A PROACTIVE APPROACH

ON THE RADAR OF THE C-SUITE

All companies connected to the internet are vulnerable to cyber-attacks. And the potential losses are significant. With increased scrutiny placed upon managing potential cyber security risks, it's more important than ever to implement a robust vulnerability management program. This report discusses different aspects to vulnerability management from the perspective of a Chief Information Security Officer (CISO).

All companies connected to the internet are vulnerable to cyber-attacks. Against a background of increased executive-level concern for cybersecurity, organizations are seeking to ensure the protection of their information assets and minimize the risk of a cybersecurity attack. More and more organizations have appointed a CISO to head up their information security operations.

As a CISO, you navigate between the strategic, tactical and operational level of information security management every day. One of the most important skills you must master is communications. In addition to managing the day-to-day cyber security operations of the company, it's your job to ensure that senior executives and board members are appropriately informed of the organization's security status. In this report, we'll give you valuable insights on how to get vulnerability management right, and how to effectively present the related risks and priorities to other company decision makers.



ON THE RADAR OF THE C-SUITE

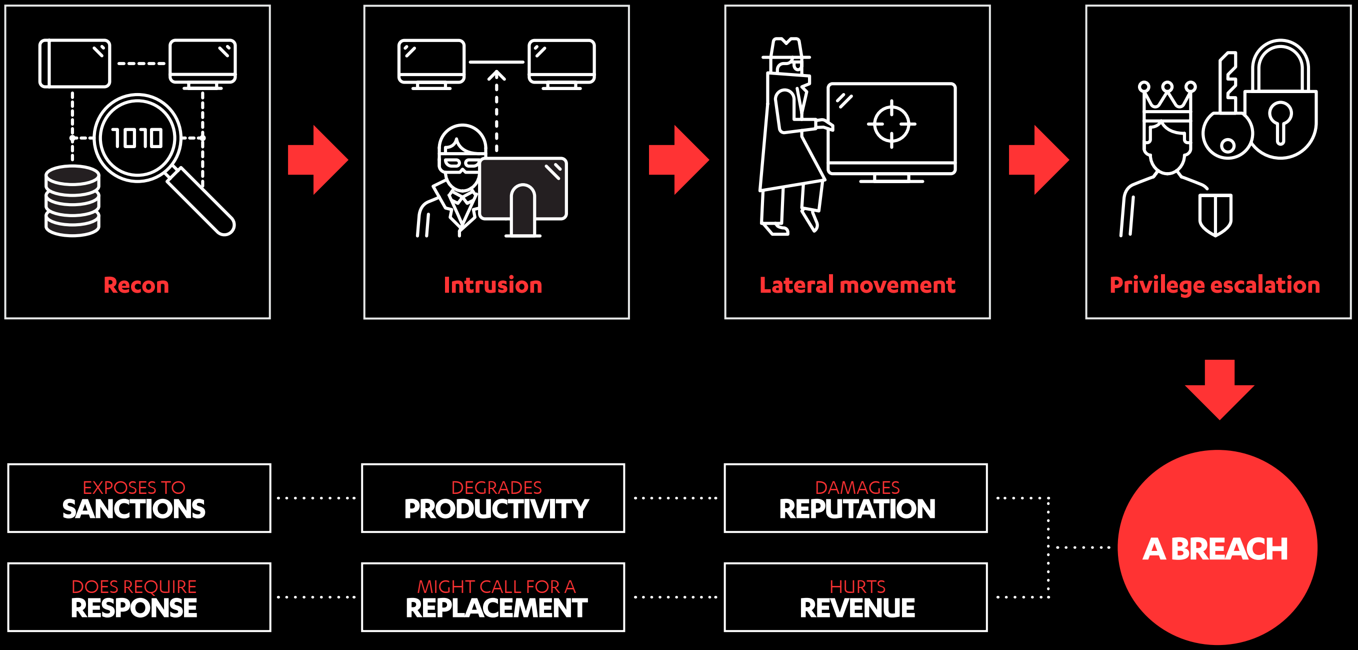
According to a recent Forrester Global Security Survey, 49% of organizations had suffered one or more breaches in the past year. Data from Forrester also shows that software vulnerabilities are the single largest factor in enterprise breaches. According to the survey, of all organizations that reported being breached in the past year, 56% had experienced a breach as an external attack, and the number one issue that was pervasive across the attacks was software vulnerabilities or software exploits.

Having helped numerous companies recover from security incidents, we've seen firsthand the damage a single vulnerability can cause, as well as how easily some breaches could have been avoided. Vulnerability management has been around for a long time, and if there's one thing we've learned from the incident response cases we've worked on across the globe, practically every attack still involves an exploited vulnerability.

Companies are increasingly realizing that cyber security is not just a technical problem, but a business risk. The impacts of data breaches are diverse. A breach can expose your intellectual property and other confidential data, and compromise your customers' private data. Data breaches can undermine customer trust, degrade productivity, endanger revenue growth and profits, and permanently hurt your company's brand and reputation.

High-profile breaches have made everyone conscious of cyber security issues, and as awareness and knowledge have grown, leadership teams and boards have begun to take a direct interest in the security of the companies they lead. Given that there are very real monetary and reputational consequences to a security breach, company boards and executive teams want to know what steps you are taking to prevent one.

ON THE RADAR OF THE C-SUITE



Recon

Intrusion

Lateral movement

Privilege escalation

A BREACH

EXPOSES TO **SANCTIONS**

DOES REQUIRE **RESPONSE**

DEGRADES **PRODUCTIVITY**

MIGHT CALL FOR A **REPLACEMENT**

DAMAGES **REPUTATION**

HURTS **REVENUE**

ON THE RADAR OF THE C-SUITE

Liability for data breaches that affect customers leads directly to the C-suite. Executives need to know how strong their company's cyber defenses are, as well as the expected responses for cyber-attacks or breaches. For a CISO, this means that it's crucial to gain the full picture of how an attacker would target you and what does your organization's entire attack surface encompass, and then translate that into risks, opportunities, and actionable strategies that you can communicate to all the executives that are involved in making decisions around securing your organization.

The C-suite and its functional teams need more education, understanding and engagement in order have an appropriate, risk-aware posture that helps protect company assets, reputation and the broader business ecosystem. To begin, many executives require briefings so that "cyber security" is demystified and better understood. Business leaders will increasingly demand clarity around the security risks that their organizations are exposed to, and how secure they are in response to those risks – particularly around compliance issues. Alongside this, they will require ongoing monitoring and board level reporting. This means that CISOs will need to deliver clear-cut reports and action plans to tackle the risks. The stakes are high. What is needed is a solid structure for monitoring and managing cyber risk in the company.

> "Cyber security is a constant battle for every business, and one of the challenges in many organizations is getting the executive teams to understand that enterprise-wide risk management is more than an IT problem."
>
> Erka Koivunen, CISO
> F-Secure Corporation

THE FOUNDATION OF A SOLID CYBER SECURITY PROGRAM

Vulnerability management is a foundational process in any information security program and regulatory compliance framework. From our investigations, we know that most companies fall victim to attackers either because of unpatched software with known vulnerabilities, or because of the human factor, for example people falling victim to phishing emails.

A new security vulnerability is identified every 90 minutes, and several thousands of vulnerabilities are disclosed every year. On average, it takes 103 days for a vulnerability to be remediated.* In contrast, according to Gartner, the time it has taken from a patch coming out to when an exploit appears in the wild has dropped from 45 days to 15 days during the past decade. Gartner notes that, on average, vulnerabilities that are exploited at day zero (aka with no knowledge of the vendor or no prior remediation being available) are about 0.4% of total vulnerabilities each year during the past decade.

So, as much as we talk about and focus on zero-day attacks, the reality is that these types of undisclosed vulnerabilities and subsequent exploits make up only a small percentage of the vulnerabilities being exploited today. In reality, the primary method of compromise is still the exploitation of known but unmitigated vulnerabilities, and the majority of attacks exploit known vulnerabilities for which a patch was already available. In other words, companies still struggle with old vulnerabilities from years past. The 2016 Verizon Data Breach Report looked at CVEs exploited in 2015, and found both 2015 CVEs, but also ten year old and even seventeen year old CVEs being exploited successfully.

We are starting to see this realization reflected in enterprise security spending. In the recent Forbes Insights security survey, 60% of the 300 C-level respondents said that “expanded vulnerability discovery and remediation” was a primary initiative for them in 2016. In contrast, only 30% of the respondents stated that putting more resources into defending against zero-day exploits was a priority. This is a logical response considering that the vast majority of exploits are still targeting known vulnerabilities that can either be easily patched or fixed.

CASE: WANNACRY

The massive WannaCry crypto-ransomware outbreak is the most recent example of a known vulnerability being exploited to great effect. In May 2017, the WannaCry ransomware spread across the globe, infecting systems and disrupting a wide range of sectors including transportation and health services. The outbreak was based on a Windows Server Message Block (SMB) vulnerability, MS17-010, that had been patched by Microsoft in March. However, many were still behind on patches or were running legacy operating systems such as XP which are no longer supported nor updated with security patches. Due the size of the outbreak, Microsoft provided a patch also for XP and Server 2003.

The spread of the worm would have been reduced had more systems been kept up to date. Telemetry from F-Secure's vulnerability management tool, Radar, indicates that 15% of hosts run Windows SMB. The WannaCry outbreak dramatically illustrates why admins should make sure SMB is properly patched and is not exposed to the public Internet.

In general, our recommendation to companies is to have a continuous, comprehensive vulnerability management program that allows organizations to promptly detect flaws and weaknesses in their systems and prioritize remediation so that the most critical issues get patched or mitigated in due time.

THE FOUNDATION OF A SOLID CYBER SECURITY PROGRAM

Vulnerabilities that are ranked medium severity dominate organizations' network vulnerabilities. The CVE Details website shows an average vulnerability score of 6.8 across all known vulnerabilities, on all known platforms. Of the over 80,000 known vulnerabilities in their database, 12,000 (~15%) are classified as high-severity. Remember, though, that these vulnerabilities exist over plenty of different client and server-side applications (including, you guessed it, Adobe Flash). And if we analyze vulnerability trends within our customer base with F-Secure Radar, it shows pretty much exactly this. High severity vulnerabilities were rare to non-existent. The vast majority of unpatched vulnerabilities we found were of low-medium severity.

From a company's point of view, handling high-severity vulnerabilities is a number one priority, and they get handled in well run organizations. Of course, it makes perfect sense that you're going to perform triage when a new high-severity vulnerability surfaces. But what about the rest of them?

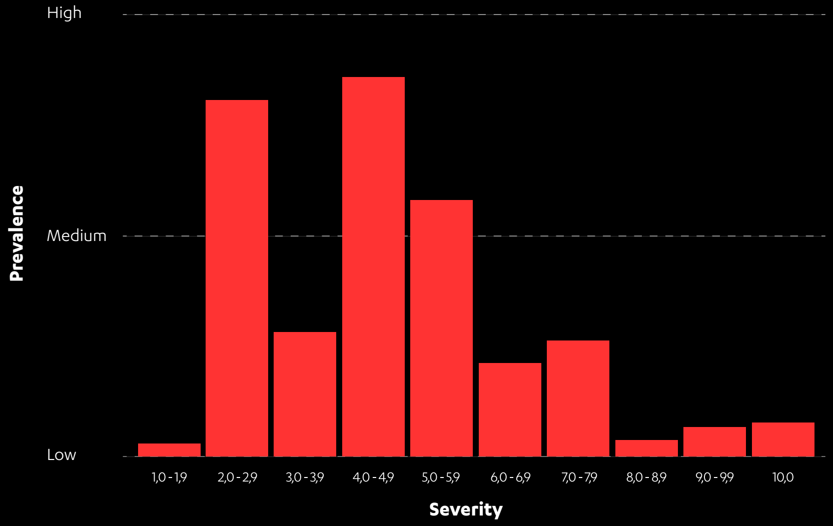
Applying every patch to every piece of software on every system on your network when a patch is released is just not feasible. That's why admins rely on periodic patch cycles to fix low severity vulnerabilities, if they do at all. Companies should focus primarily on fixing the vulnerabilities they know exist. While these vulnerabilities are easy to ignore, they're also easier and more inexpensive to fix than to mitigate later on.

With new threats arising every day, managing vulnerabilities and staying ahead of risks can feel like treading water. There's always a new vulnerability to address, a patch to apply, security tools to evaluate, and defenses to update. Taking time out of your day to understand the implications of every newfound vulnerability out there, prioritize them and plan for patch management seems like a lot to ask, but is well doable with the right combination of human expertise and advanced solutions.

THE FOUNDATION OF A SOLID CYBER SECURITY PROGRAM

	Vulnerability type	Average Severity
1	SSL configuration	●●●●○○○○○○
2	SSH	●●●●●●○○○○
3	Web servers	●●●●●●○○○○
4	SSL Certificates	●●●●●○○○○○
5	Management interfaces	●●●●●●○○○○
6	SMB	●●●●●●○○○○
7	Application	●●●●●●○○○○
8	Linux	●●●●●●●○○○
9	CGI	●●●●●●○○○○
10	SSL implementation	●●●●●●○○○○
11	Windows	●●●●●●●●○○
12	Databases	●●●●●●●○○○
13	Web applications	●●●●●●○○○○
14	FTP	●●●●●●○○○○
15	Virtualization	●●●●●●●○○○
16	SNMP	●●●●●●○○○○
17	Application servers	●●●●●●●○○○
18	CISCO	●●●●●●●○○○
19	SMTP	●●●●●●○○○○
20	Unix	●●●●●●○○○○

20 most common vulnerability types found by F-Secure Radar



The prevalence and severity of vulnerabilities collected during 2016, over F-Secure's customer base, with our Radar product.

PART II: AN ONGOING PROCESS

SCANNING

Just like cyber security, vulnerability management is a continuous process. Companies that take cyber security seriously run a robust vulnerability management program that includes multiple scans per year, comprehensive reporting on risk, as well as detailed tracking and remediation. Here's a roundup of the essentials.

Vulnerability management is more than running a vulnerability scanner and remediating the resulting vulnerabilities on an annual basis. Only constant scanning and ruthless control can help you find vulnerabilities before anyone else does.

The frequency at which vulnerability scans are performed should be determined based on the organization's risk appetite and any applicable regulatory requirements. Performing only a single vulnerability scan each year puts companies at risk of not uncovering new vulnerabilities early enough. This period of limbo is all an attacker needs to compromise a network.

The Payment Card Industry Data Security Standard (PCI DSS) demands organizations that process payment card data to run internal and external network vulnerability scans at least quarterly and after any significant change in the network. In addition, the European Union General Data Protection Regulation (GDPR) that enters into force in May 25, 2018 will incentivize companies to invest in proactive measures to secure personal data.

With an advanced vulnerability management solution, you can create standardized and custom report. The reports will help you prioritize patch management and other remediation efforts, and they can also be used to show that you're proactively investing in predicting and preventing threats and demonstrate that you're compliant with the latest regulations such as PCI-DSS and EU GDPR.

SCANNING

Map your IT assets

To achieve a comprehensive view of your continuously changing IT environment, you need active mapping and monitoring of your assets. Otherwise, your vulnerability management decisions will be based on incomplete or inaccurate information, which puts your organization at an elevated risk of breaches.

Identify vulnerabilities

Scan your systems to identify security vulnerabilities associated with configuration errors, improper patch management, implementation oversights, and more. As a result of the scans, you should get a prioritized list of vulnerabilities to patch as well as clear recommendations for remediation.

Scan your web applications

Web scanning allows you to detect vulnerabilities in commercial and custom-built web applications. In addition to regular scanning of existing applications, we recommend you to use web scans during the development of new web applications as part of the development life cycle.

WEB TOPOLOGY MAPPING

Rapidly changing, complex business IT environments lead to a broad attack surface. In addition to scanning for vulnerabilities in internal systems and applications, forerunning organizations have visibility to shadow IT. They map their full attack surface – including enumerating outside-in attack vectors with an Internet and web threat assessment – and respond to critical vulnerabilities associated with cyber threats.

Gartner predicts that by 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources. Business units deal with the reality of the enterprise and will engage with any tool that helps them do the job. Companies should find a way to track shadow IT, and create a culture of acceptance and protection versus detection and punishment.

When you're looking into including web topology mapping within your vulnerability management program, the capabilities you should look to build include:

- **Detecting orphaned or shadow systems** (shadow IT) and identify potential risk concentration and unintended interdependencies
- **Detecting malware-infected websites**
- **Identifying assets** that are closely connected to you through hosts linked to your organization's websites
- **Monitoring phishing and brand infringements** to protect your brand and intellectual properties against fraudulent or malicious activities
- **Auditing your service providers' security practices**, in cases where your own security policies differ from those of a partner.

WEB TOPOLOGY MAPPING

Information Security

Your InfoSec department will probably be most interested in web topology mapping. Members of the IT department, security experts, incident response teams, and crisis management teams all need access to up-to-date threat surface assessment reports.

Threat Assessment and Pen Testers

Anyone in your organization tasked with running threat assessments, network security assessments, or penetration tests will find web topology mapping invaluable, especially when combined with other tools on the market.

Legal

Legal would appreciate a service capable of monitoring for brand infringement or other fraudulent activities related to your company's brand or intellectual property.

Marketing and Business Development

A web topology mapping service designed to monitor and report on referrers will allow your sales, business development and marketing guys to identify potential opportunities, and monitor for brand infringements.

PRIORITIZATION

The vulnerabilities resulting from scans can be numerous and overwhelming. The challenge when dealing with high volumes of vulnerabilities is how to prioritize them. Many of the vulnerabilities we think need to be addressed right away may in fact be gaining attention based on media hype or other external factors, not necessarily based on the severity of the impact to your organization. While a vulnerability may be real, the actual business impact of a specific vulnerability to your company may not be clear.

Vulnerabilities should always be prioritized based on risk, and organizations need to address their vulnerability management in a structured manner so that they are progressively working through managing their own vulnerabilities – rather than getting distracted by the latest news in the industry.

No vulnerability management tool can give you a silver bullet in the fight against various cyber threats. It takes human expertise to turn the reports generated by vulnerability management software into a prioritized action plan. The solutions may classify vulnerabilities and guide you, but no vulnerability management solution will decide for you which vulnerabilities to patch first. This is where the expertise of IT security professionals comes into play.

> “For most IT admins, taking time out of their day to understand the implications of every newfound vulnerability out there is too much to ask for.”
>
> Andy Patel,
> Cyber Security Expert,
> F-Secure

REMEDIATION

Once you have prioritized the vulnerabilities, they must be remediated. Otherwise, what was all the work for? The list of discovered vulnerabilities can range from a single page to a lengthy novel. However, it's very common to find that a single remediation task will resolve multiple vulnerabilities within the list. You don't have a lot of options; either remediate the issue, ignore it, or apply other measures (compensating controls) to mitigate the risk posed by the vulnerability.

You may not be able to patch everything in each cycle, but you need to make sure that you base your decisions on risk-based reporting and can always justify why some vulnerabilities were patched while others weren't. Once you have all this on paper, you are limiting the liability of both yourself and your company in case your company would get breached through an exposed vulnerability despite swift vulnerability remediation.

As a CISO, you should also carefully track all remediation efforts and follow organizational change management procedures to ensure no vulnerabilities are overlooked. Upon completion of remediation efforts, the network should be reassessed to ensure all discovered vulnerabilities have been resolved and that new vulnerabilities have not been introduced.

PART III: SMARTER VULNERABILITY MANAGEMENT

WHAT TO LOOK FOR IN YOUR VULNERABILITY MANAGEMENT SOLUTION

When you're looking for effective vulnerability management, you need to make your decision based on hard facts. So make sure your vendor can answer "Yes" to all of the points below. And if they can't, look for one that can.

- **COMPREHENSIVE VISIBILITY**
  Effective security mapping through precise discovery and mapping of all assets, systems, and applications on the network and beyond.
- **STREAMLINED PRODUCTIVITY AND SECURITY MANAGEMENT**
  No more inefficiency and missed security risks. Quickly address problems across multiple domains with an efficient service workflow, including vulnerability monitoring, automated scheduled scans, and ticketing for prioritized remediation and verification.
- **REPORTING ON RISK**
  Produce reports with credible information about your organization's security posture over time. Show and justify how IT security enables business continuity.
- **REDUCED COSTS**
  Vulnerability management is an opportunity to significantly lower the cost of security. It's less costly to deal with security before serious problems arise than it is to deal with it during a crisis or incident recovery. Additionally, leveraging Radar's cloud resources allows organizations to lower their expenses.

> "The best way to handle cyber threats is to actually foresee them by fixing vulnerabilities before they can even be exploited. This means hardening an organization's entire attack surface."
>
> Jimmy Ruokolainen,
> Vice President,
> Product Management,
> F-Secure

WHAT TO LOOK FOR IN YOUR VULNERABILITY MANAGEMENT SOLUTION

Cyber security isn't simple. And it's not something you can ever call "done". So unless you continuously improve your security capabilities, you won't be able to protect your business against emerging threats like ransomware – and whatever comes next.

Whatever the size of your business, being aware of the risks and prepared to battle new threats is essential. And it all starts with effective vulnerability management. But remember: vulnerability management is just one part of a big puzzle. You need a holistic approach to cyber security that covers all the aspects of prediction, protection, detection, and response.

It's less costly to deal with security before serious problems arise than it is to deal with it during a crisis or incident recovery. Shore up your defense with vulnerability management already today — this is too important to wait.

LIVE SECURITY: A CONTINUOUSLY IMPROVING APPROACH

To deal with the relentless innovation in the threat landscape and your corporate infrastructure, you need to make sure your security technology is continuously improving.

Live Security is an approach to cyber security that uses the continuous influx of tactical threat intelligence from out in the field to constantly improve technology that can scale to protect all your endpoints.a

Read our SlideShare to find out what it's all about and why you should think seriously about it. Live Security is an approach to cyber security that uses the continuous influx of tactical threat intelligence from out in the field to constantly improve technology that can scale to protect all your endpoints.

Discover smarter vulnerability management

See what intelligent vulnerability management really looks like—and why the combination of man and machine is so vital for staying one step ahead of attackers. Learn more

WE'RE F-SECURE

For too many businesses, too many manufacturers, too many people, security is an afterthought. What's the use of being connected to everything if our data, our identities and our transactions aren't secure?

From more than twenty-five years of protecting millions of computers around the globe, from the first malware to the latest targeted attack, we know this for sure: you will be hit. The only question is if you will recover and come back stronger.

To do that, you need the right team in your corner. For F-Secure, cyber security is more than a product—it's how we see the world.

Read our Business Security Insider blog to get the latest from the frontlines of the industry. Or better yet, if you're looking for a cyber security partner that always keeps you one step ahead, we should talk.

f-secure.com

F-Secure.

SOURCES

[1] Forrester Vendor Landscape: Vulnerability Management, 2017 https://www.forrester.com/report/Vendor+Landscape+Vulnerability+Management+2017/-/E-RES136784

[2] https://www.tenable.com/blog/2017-trends-in-vulnerability-management-featuring-forrester-research

[3] Nopsec, 2016 Outlook: Vulnerability Risk Management and Remediation Trends

[4] Gartner, It's Time to Align Your Vulnerability Management Priorities With the Biggest Threats, Craig Lawson, 9 Sept 2016

[5] The 2016 Verizon Data Breach Report

[6] Forbes Insights – Enterprises Re-Engineer Security in the Age of Digital Transformation

[7] http://www.cvedetails.com/

[8] http://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/