REPORT

GoSecure CYBERSECURITY PERCEPTIONS VERSUS REALITY

INTRODUCTION

Organizations of all types and sizes are under attack. Unfortunately, there seems to be a disconnect between defenders' perceptions and practices of how best to protect themselves and the current cyberthreat landscape -or more precisely- the most common attack vectors leveraged by penetration testers acting as potential attackers. It is a classic case of perception versus reality.

To begin distinguishing perception from reality, we developed a survey, in collaboration with Serene-risc, a knowledge mobilization network in cybersecurity based in Canada, on the perceptions and practices of cybersecurity professionals. The survey aimed at understanding how defenders perceive specific security measures and whether these measures were implemented in their respective organizations. Combining the survey results with our penetration testing experience, we confront two perspectives: the defenders' and the pentesters', the latter standing as proxies for real attackers. This report highlights the main findings of the study and provides a handful of pro tips in order to overcome the security gaps uncovered.

This report contains three sections. The Overview provides a quick description of the data as well as a review of the survey population. Section 1 then explains the key results of the survey and compares them with our pentesters' experience. As expected, we find incongruities between our understanding of the cybersecurity landscape and what is reported. In Section 2, we dig further by linking defenders' perceptions with their reported actions, cross-referencing the results with statistics on penetration testing. Here, we uncover some potential biases in the defenders' mindset.

In the end, this study shows how defenders can overcome information gaps and biases by building their security practices so that penetration testing engagements fail. By doing so, it is likely that real attackers will be defeated more often.

QUICK OVERVIEW OF THE DATA

For transparency purposes, a description of the survey population, as well as GoSecure's penetration team and the sample of penetration testing reports used, are presented below. Moreover, the survey data is available online at: https://www.serene-risc.ca/en/survey-perceptions-vs-reality

SURVEY POPULATION

A total of 120 respondents answered the survey. Among the respondents, there is a good cross-section of titles representing everything from management level jobs (including CEO, CTO, CISO) to hands-on professionals, such as dedicated security analyst/architect, management, network administrator, senior infrastructure analyst, security administrator, and system administrator. As shown in Figure 1, a total of 50.8% of respondents occupied a management level position (including C-level positions). Thus, a large part of the sample encompasses individuals with decision-making capabilities in their organization.

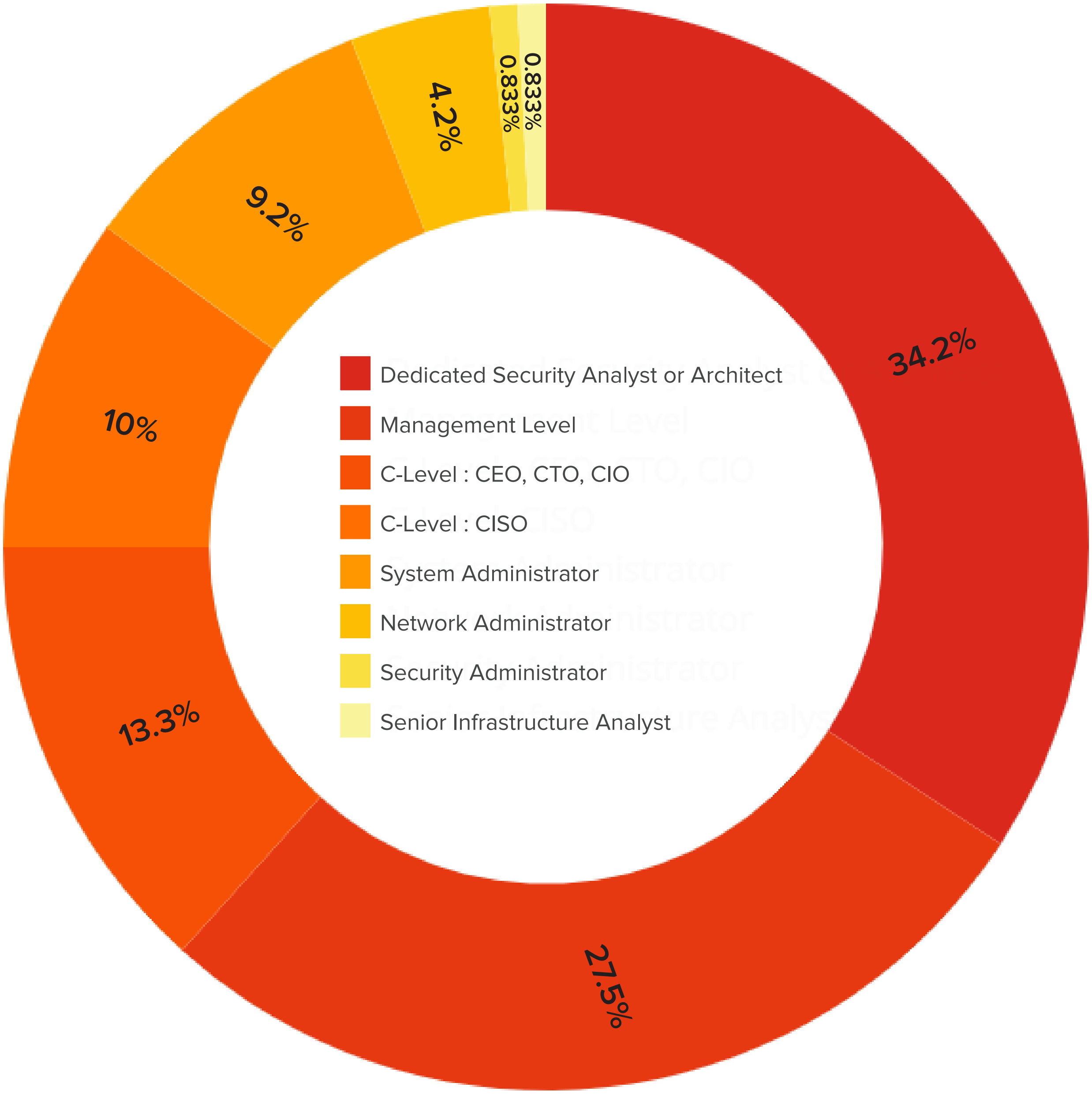


Figure 1– Survey Respondents' Position in their Organization

In terms of experience, 49.2% reported having more than 10 years of experience, 25% between 5 to 10 years and 25.8% less than 5 years, as shown in Figure 2.

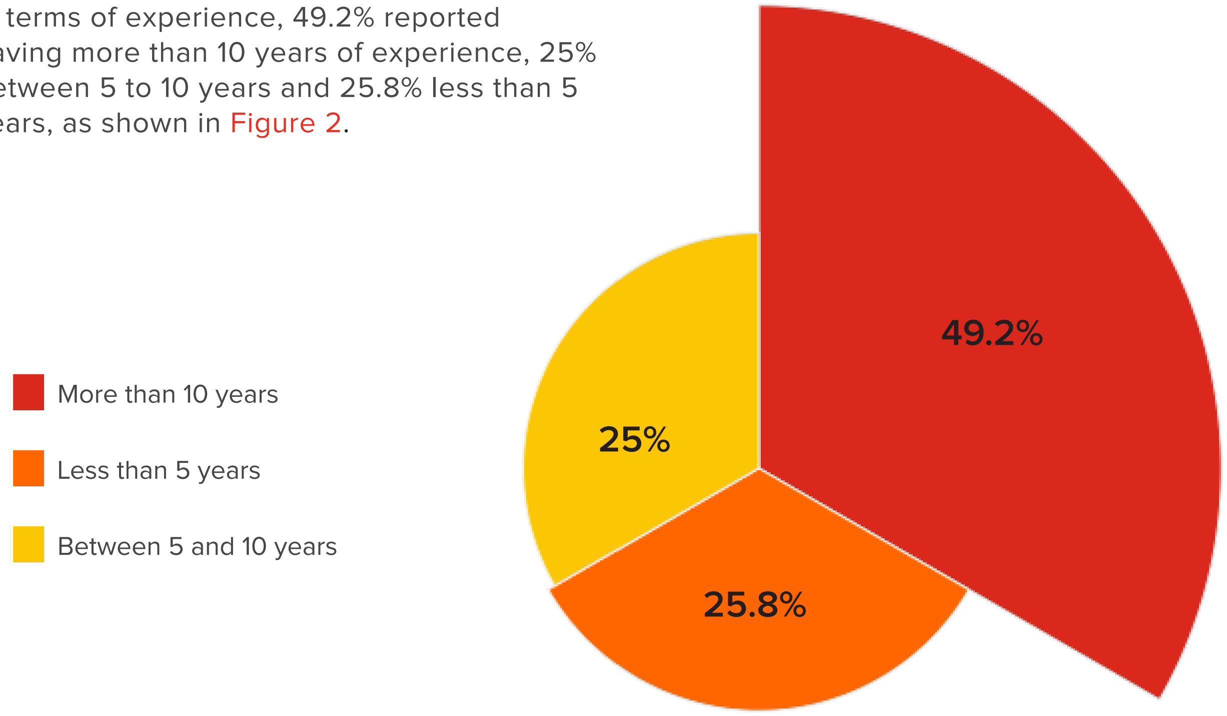


Figure 2 - Respondents' Experience in Years

A total of 64.1% of respondents also reported being employed in an organization with more than 500 employees and 84.8% were based in Canada or the United States.

For those interested in investigating the results further, the microdata of the survey is available online.

PENETRATION TESTING EXPERIENCE

GoSecure has extensive experience conducting internal, external, and Web application penetration tests, as well as red team engagements and social engineering assessments, performing hundreds of tests across North America every year. The clients tested operate in various sectors, such as banking, transportation, retail, aviation, and their sizes range from small to international corporations. The statistics on penetration testing findings in Section 2.2 include 65 reports (engagement type: internal, external, and Web applications) from which 182 findings are extracted.

PART 1:
CONFRONTING DEFENDERS AND ATTACKERS

This survey sought to assess the perceptions and practices of cybersecurity professionals towards different aspects of the security posture of their organization. In this section, we present key results from the survey related to multi-factor authentication, password policies, specific security measures, patch management, products' features enabled by default, asset inventories, and endpoint visibility. In each subsection, the results of the survey are compared with the experience of penetration testers and followed by pro tips to remedy the information gaps found.

1 - MULTI-FACTOR AUTHENTICATION

Respondents were first asked about multi-factor authentication (MFA), a security measure requiring that a user presents at least two factors, such as: "something that you know" and "something that you have", before being granted access to a system. When asked, on a scale from 1 to 5, how important multi-factor authentication is for the security of their organization, 93.3% said important or very important.

When asked whether such a measure was implemented in their organization on their external network, 45% replied yes, 41.7% partially, and 13.3% no, as shown in Figure 3.

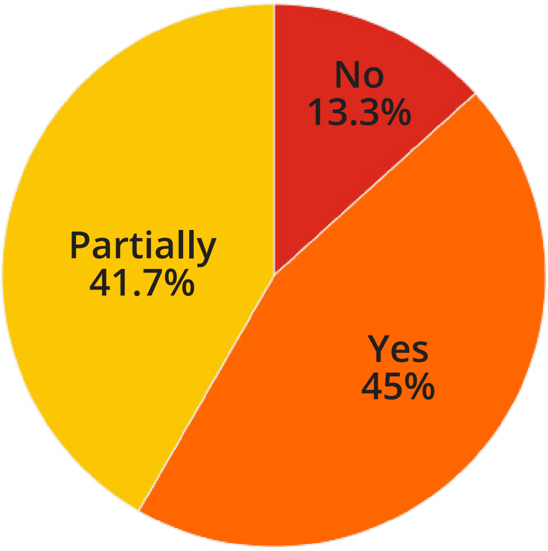


Figure 3 - Multi-Factor Authentication at the External Perimeter

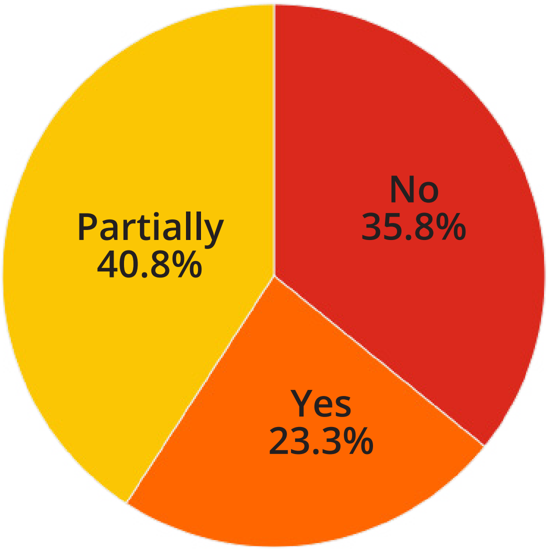


Figure 4 - Multi-Factor Authentication at the Internal Perimeter

When asked if multi-factor authentication was implemented on their internal network – a measure that could prevent an attacker who has breached a system to pivot internally in the organization to more valuable assets – the response distribution was more conservative, as shown in Figure 4. A total of 23.3% of respondents mentioned that they fully implemented multi-factor authentication on the internal network, 40.8% partially and 35.8% said that they did not implement this security measure.

PENETRATION TESTING EXPERIENCE

Penetration test results show that multi-factor authentication is very efficient for blocking attackers. However, such a measure must be implemented on all externally exposed services, not only the email service, the most common MFA location. Moreover, it is important to note that a secret question is not a second factor: a password and a secret question are both based on a user's knowledge. Each factor must come from a different authentication vector: a password is what one knows, and an RSA OTP number is what one has, for example.

Moreover, GoSecure pentesters were surprised that 23% of the respondents said that they implemented multi-factor authentication on the internal network, as they have rarely encountered such security measures in organizations internally. They added that even if critical services have two-factor authentication, day-to-day activities are usually unprotected, such as RDP access to servers or file share access.

PRO TIPS ON MULTI-FACTOR AUTHENTICATION

- Focus on implementing autentification.
- SMS-based multi-factor authentication is better than single-factor authentication.

  Keep in mind that for critical services that could be targeted by highly motivated attackers, SMS-based multi-factor authentication could be bypassed using a technique called SIM Swapping
- An affordable multi-factor authentication solution is the use of software tokens. These rely on an application on your phone or a computer containing a secret feed instead of relying on a physical token like an RSA key. This is one of the cases where open source solutions exist, but their management and integration are relatively complex. You might consider using a commercial solution if ease of implementation is a concern.

  Be aware that the information sent to the user to enroll the token can sometimes be reused by an attacker if the attacker gets access to it. Thus, it is important to encourage users to destroy the file or email once they have registered their software token.

2 - PASSWORDS POLICIES

The importance of having a good password policy is well-known across the industry. When asked to select the minimum requirements for a good password policy, 56.3% of respondents mentioned that passwords need to be at least six characters long and 74.8% said that they need to be a mix of letters, numbers, and special characters. Moreover, a total of 83.1% agreed that password reuse should be prohibited, 81.5% agreed that known popular passwords should also be mitigated for and 62.2% said that dictionary words should be forbidden.

Interestingly, we noticed two trends in the data regarding regular password changes: 43.7% agreed that regular password changes (such as every 90 days) should be a minimum requirement while another 43.7% of respondents said the opposite: no or few password changes (once or twice a year or at the suspected compromise of passwords) should be the minimum requirement. Some people also selected both options.

This discrepancy in the results can be explained by the idea that mandated password change is a double-edged sword: it can mitigate a potentially compromised password, but also seems to be disliked by users, who end up finding simpler passwords or incrementing a number to their previous passwords to bypass this security policy. "Human acceptance" of a security feature is essential for it to be efficient: if end users do not like the security controls, they will always find a way to bypass it. Below you will find a good -and unfortunately true- story, told by one of our pentesters, on how a user had bypassed a password security feature:

"The password policy was preventing users from setting passwords that were used previously. Any of the last 6 passwords were blocked. To circumvent this policy, users could change their passwords six times in a row (within a short time window) and get back to their favorite password. One person did this every three months so that the password would always be the name of his/her cat."

Moreover, respondents were asked if the organization they worked for, as security specialists, met the minimum password policy requirements that they had just selected. The distribution of responses is shown in Figure 5 and illustrates that 17.2% said no, 23.3% said partially, and 59.5% said yes. Although quite optimistic, this goes against all our pentesters' experience, as explained in the discussion below.

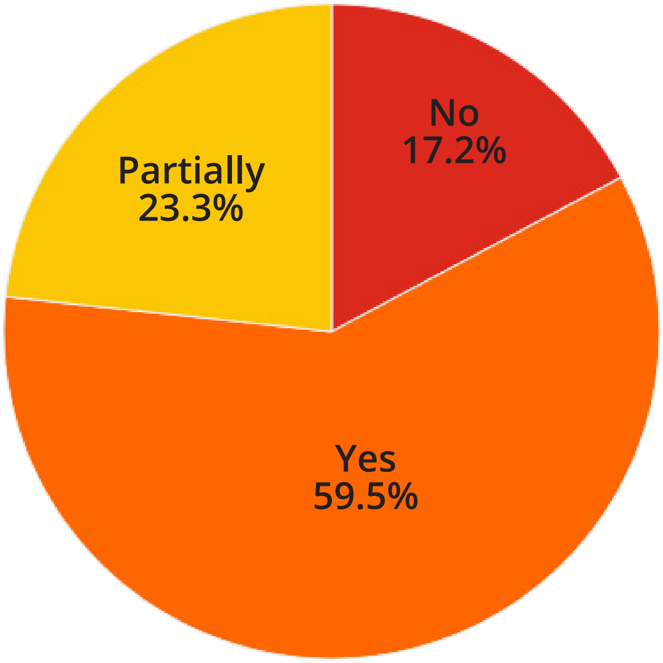


Figure 5 - Organization meeting password minimum requirements set by respondents

PENETRATION TESTER EXPERIENCE

Penetration testers often use two techniques to compromise systems with passwords: password spraying and password cracking. Password spraying consists of trying a popular password on a large number of accounts and finding the weakest link: the account with THE guessable password. Generally, when conducting such attacks, pentesters have a list of "all-star passwords". This list includes simple passwords like *Password123, Welcome1, Letmein1, SeasonYear,* and *Companyname123*. When conducting password spraying on companies, pentesters reported being successful, on average, 25% of the time. Password cracking, on the other hand, requires that pentesters have access to a list of encoded/hashed passwords (possible through various attacks such as LLMNR spoofing) and try to find the plain text password by encoding/hashing a known list of passwords and testing them against the compromised list. In such situation, pentesters find, 20% of the time, passwords with: name and four numbers, such as *Julia1984*, 4-5% of the time, passwords with vulgar words (you can probably guess examples) and 4-5% of the time passwords with vacation words in them, such as *BeachCuba1*. When performing password cracking, pentesters have reported being successful in finding at least one password most of the time.

Moreover, in password audits where they try to crack the password hashes from a database of user accounts, usually found during a penetration test, they reported having been able to recover up to 98.3% of an enterprise's passwords. This is made possible and relatively affordable due to the enormous advancements in Graphical Processing Units (GPUs) over the last decade which are leveraged for password cracking.

Thus, when 60% of respondents say that their company meets the minimum requirements for good password policy, it seems to be a mismatch with our pentesters' experience. This may be because passwords such as CompanyName2019* do meet requirements for good basic password policy, but penetration testers are aware of these different variations and leverage them when cracking passwords. Moreover, the likeliness of one user having this password in a large pool of users is high.

PRO TIPS ON GOOD PASSWORD ENFORCEMENT PRACTICES

- Block any words related to the company (with a password filter, for example), even though special characters or numbers are added to the password. If needed, you can use Microsoft's password filter feature.
- Mention to employees that passwords should not be related to information publicly available about them online on social networks, such as Facebook, LinkedIn, or Instagram. Pentesters often use such information when conducting external tests.
- When a security incident happens or an external person gets access to the active directory user database, you should enforce password changes on the whole network, including service accounts and most importantly, the krbtgt account, the most powerful service account in the active directory.
- Continuous password auditing activities could be achieved to proactively track any potential weak passwords. For example, periodically extracting the user database, trying to crack their password hashes, and forcing password changes for all the successfully cracked hashes is an effective additional practice.

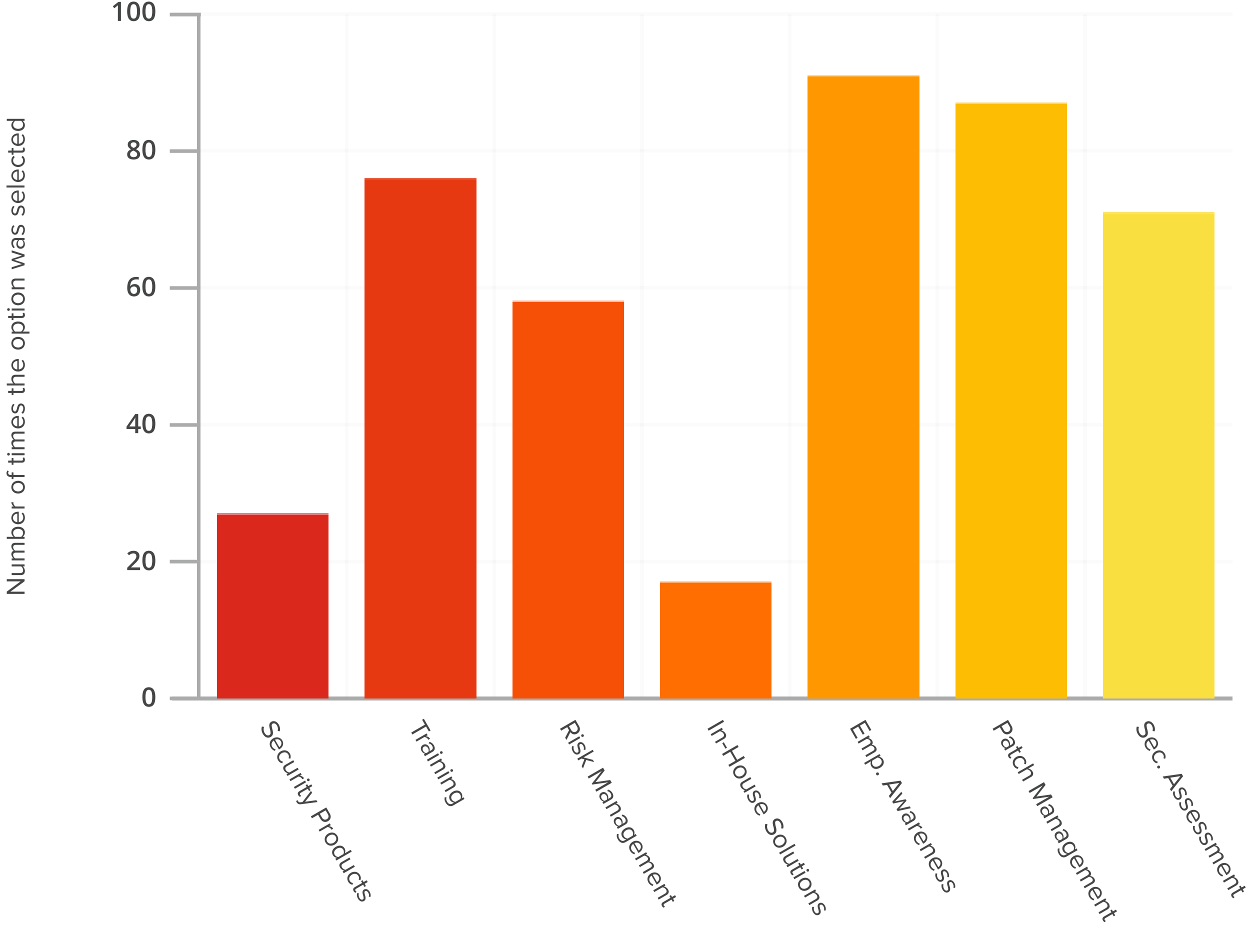
3 - SECURITY MEASURES DILEMMAS

Respondents were asked which security measures (based on a set of predetermined measures) would increase the security posture of their organization. They could select more than one measure, which included:

- Better security products (e.g. anti-virus/Firewall/WAF);
- Training of IT employees;
- Better information security risk management and policies;
- In-house development of security solutions;
- Employee security education and awareness training;
- Better vulnerability patch management and;
- More security assessments and/or testing.

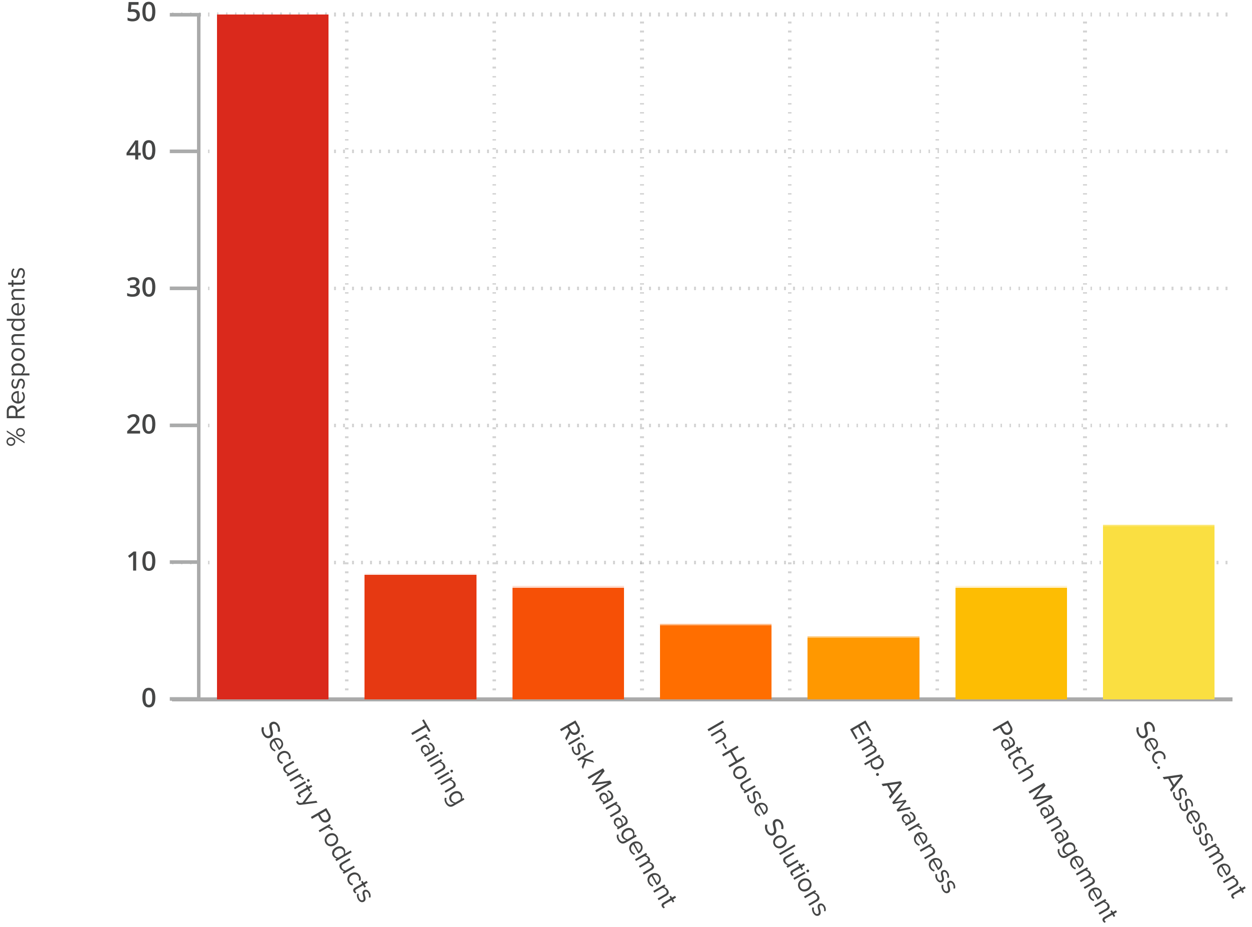
The distribution of responses is shown in Figure 6. We see that employee awareness is at the top, followed by patch management, training, and security assessments. These measures are thus considered efficient to enhance the security of an organization. Security products and in-house solutions, on the other hand, do not seem to be a popular measure among defenders.

Figure 6 - Efficiency of security measures according to respondents



Respondents were then asked to select the security measures their organization invested the most in, the results are shown in Figure 7. According to nearly 50% of the respondents, security products are the security measure that most organizations invest in.

Figure 7 - Security measure in which organization invest the most



PENETRATION TESTING EXPERIENCE

Penetration testers agree that employee awareness is important, but stress that it is not a panacea: employee awareness training is often poorly targeted, limited in time and has, most of the time, the wrong threat actors and scenarios (i.e. Nigerian princes requiring money are a time of the past, as threats evolve). Security awareness training is not necessarily ineffective, but there are many factors working against it becoming a truly viable solution.

Rather than training the general end-user population, GoSecure pentesters have found that training of IT employees is the most efficient measure against penetration attacks. Indeed, when IT professionals know how to harden servers, block the weakest links, and are aware of the emerging threats and techniques, pentesters' work is much more challenging.

GoSecure pentesters were also not surprised that security products are what organizations invest the most in. Visit any cybersecurity conference and attendees are bombarded with messaging touting the latest technology guaranteed to solve all security problems. For example, most clients that penetration testers investigated had great anti-virus/Firewall/WAF at the external perimeter, but none in the internal network. According to them, as soon as they breached a system, pivoting inside was like water flowing through cracks. Maybe the question isn't whether an organization needs more technology but whether they need to redistribute their current technology budget?

PRO TIPS ON SECURITY MEASURE INVESTMENTS

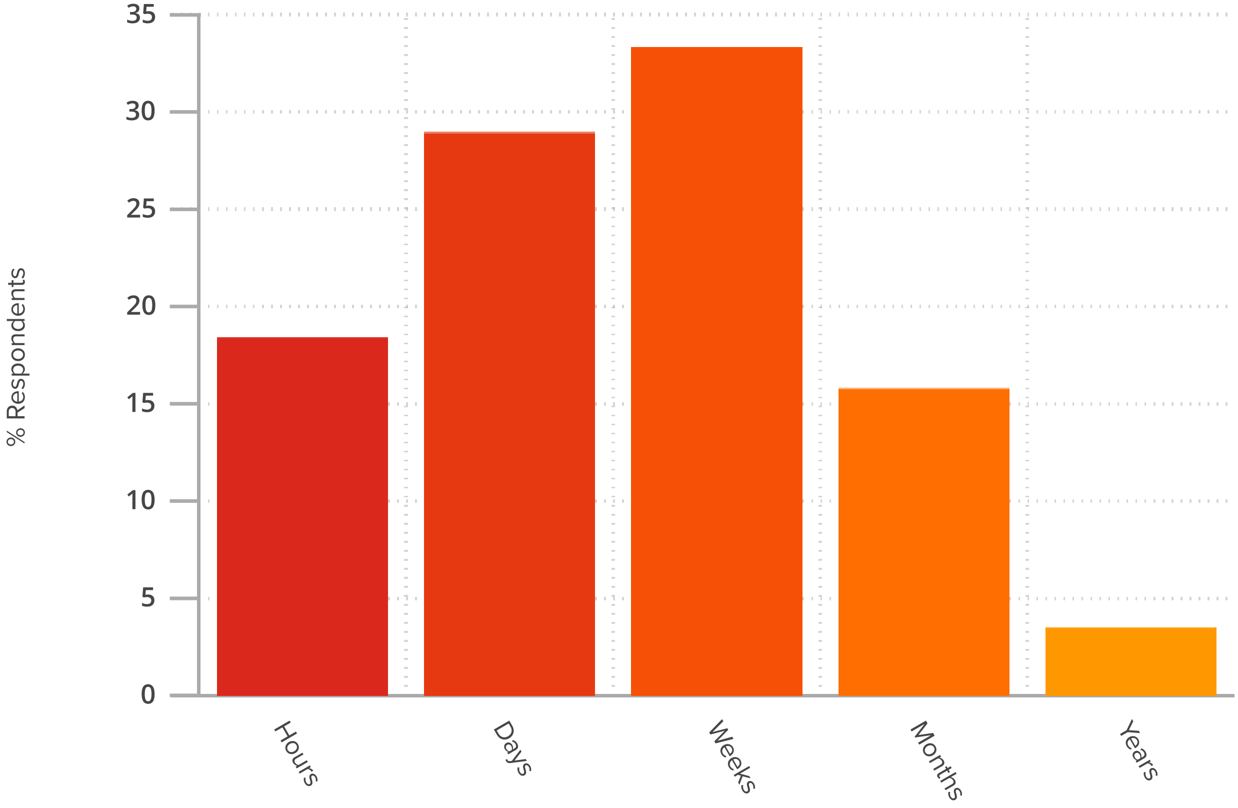
- When deciding on specific security measures to implement, consider first your company's security maturity and the technologies currently used.
- Invest in continuous training of your IT employees.

4 - PATCH MANAGEMENT

Patch management has been, in the past years, a security measure at the center of the industry dialogue: patch your systems! – is something that any cybersecurity advocate recommends. Obviously, with new vulnerabilities being disclosed every day, patching should always be a priority. When asked how important they believed patch management was for the security of their systems, over 90% of respondents said important or very important.

Asking how long it takes for their organizations to apply a security update once made available is where things get interesting. As shown in Figure 8, 18.42% said within hours, 28.95% within days, 33.33% within weeks, 15.79% within months, and 3.51% within years (yes, years). With over 52% of respondents saying it take weeks, or longer, to apply patches it's no wonder that attackers are having a field day with things like ransomware.

Figure 8 - Time required before patch management



PENETRATION TESTING EXPERIENCE

Coming as no surprise, GoSecure penetration testers mentioned that the results expressed above are in line with their experience (although they have never been aware of an IT service responding within hours to a new security update). They stressed that most of the organizations they tested had a good patch management policy for Windows updates. However, other crucial applications, such as Java, Flash or Firefox, are usually less well maintained. They can sometimes create important vulnerabilities in systems when not kept up-to-date, vulnerabilities that testers are aware of and ready to exploit.

Lastly, they still find critical vulnerabilities such as EternalBlue (MS17-010), a vulnerability patched by Microsoft in 2017, in some of the systems they test. Before engaging in a pentest, it is recommended that you perform a thorough review of all available patches (including non-Windows patches) and apply as many as possible for your organization.

PRO TIPS FOR PATCH MANAGEMENT

- Consider standardizing the tools used by your employees. For example, if your employees use Chrome, Firefox, Edge, and Opera, it is hard to patch all these browsers. Thus, in this situation, limiting the users' accessibility to a single browser could facilitate the patch management process.
- Develop a vulnerability management process that allows to identify, among others, missing patches and configuration issues.
- To minimize downtime risks caused by problematic patches performing a gradual roll-out is the current best practice. This is called a phased deployment in Microsoft's terminology.
- Use a vulnerability scanner to assess all the subnets on a regular basis to help identify and keep track of vulnerabilities on the corporate network. An open source one is OpenVAS.

5 - PRODUCT FEATURES

Many features of products are vulnerable by default and exploiting them makes the life of a pentesters so much easier! First, respondents were asked, based on their experience, how secure proprietary products (e.g. Windows, Outlook or SAP) used by most organizations are, when kept up-to-date. A total of 57.3% said secure or extremely secure, while 35.04% said moderately secure, and 7.69% said not at all secure or very limited. Then, we asked whether their organization investigated these products to identify and deactivate specific features that could represent a risk. As shown in Figure 9, 64.1% said they investigated products, while 28.2% said no, and 7.69% did not know.

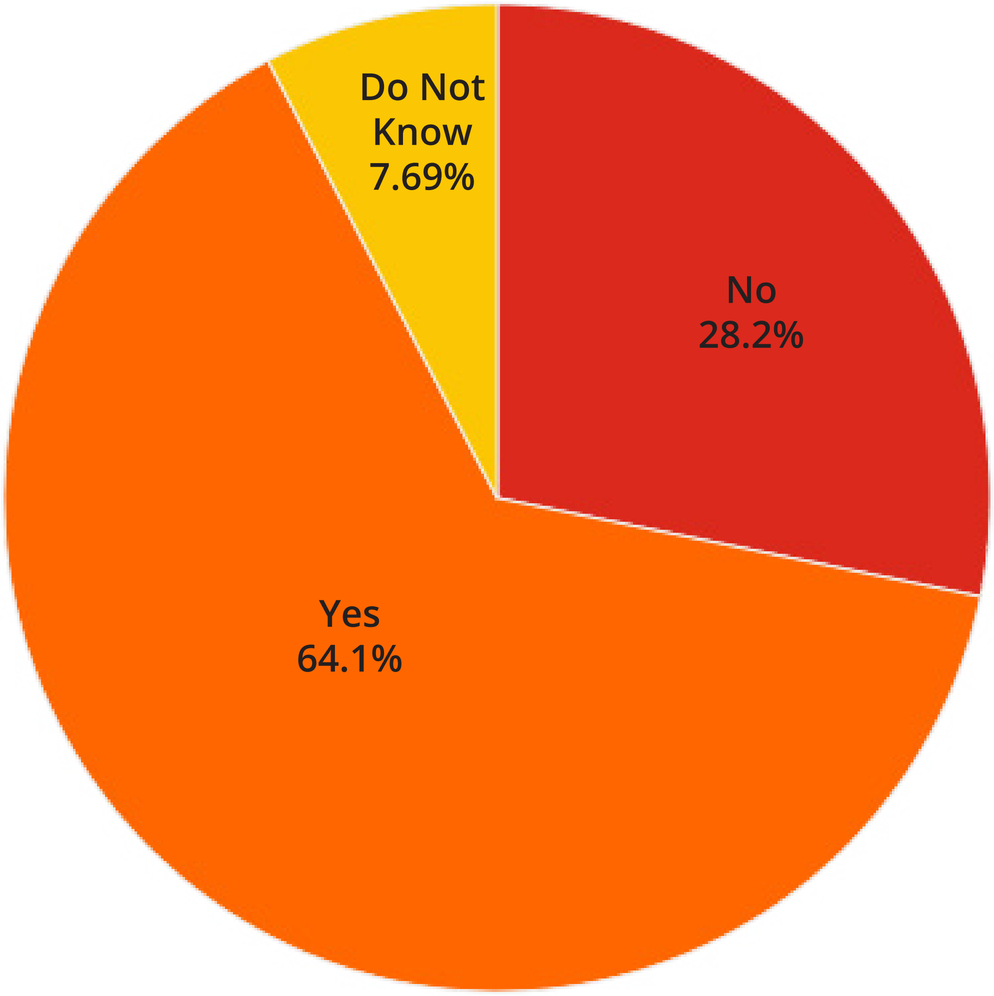


Figure 9 - Investigating Products Default Configuration

PENETRATION TESTING EXPERIENCE

Features vulnerable by default in products represent either a vulnerability (a pentester can leverage the feature to access the systems) or a missing control (an additional feature that helps pentesters in their attack process) that could be mitigated for. Overall, these features are pentesters' key attack vectors, which they, in their opinion, overuse. Indeed, they estimate that in about 80% of the penetration tests, they compromised a system via these attack vectors. Features that have rarely been seen deactivated during pentesting include: NetBIOS and LLMNR -legacy protocols that could allow the capturing of all forms of encoded credentials. Other features include but are not limited to: default passwords, Windows credentials stored in memory, unsecured DNS zones, IPV6 activated by default, and functional ARP spoofing.

Pentesters were thus surprised to find that 64% of respondents said that they mitigated that risk. Maybe they have accepted the risks associated with these features. However, -and more likely- companies may have investigated the security of a product by asking a pentest of the product or an audit, such as reviewing the product's architecture, before deployment. The product may seem very secure in security reports, but its deployment in the company's environment may be quite different than the environment in which it was first tested. Safe in a vendor's lab and safe in your environment are likely two very different forms of "safe".

PRO TIPS ON PRODUCTS CONFIGURATION

- If your enterprise uses Windows and you have no legacy operating systems (such as Windows NT) in your environment, disabling the NetBIOS and LLMNR protocols is an easy quick win for the security of your internal network.
- If NetBIOS is needed in the environment, segregate the assets that require it from the main corporate network, implement a WINS server for NetBIOS name resolution, and configure those computers to use the WINS server by pushing the corresponding registry key via GPO. Furthermore, considering the importance of this attack vector for pentesters, a strong emphasis should be put on deactivating features vulnerable by default in products. Unfortunately, an explicit list cannot be made as there are simply too many products to enumerate.
- In the long term, establish a hardening configuration standard for the different types of systems existing in the organization. The Center for Internet Security (CIS) with its CIS benchmarks, a globally recognized standard, offers extensive configuration guidelines for various technology groups.

6 - ASSET INVENTORY

Respondents were asked whether they maintained a complete inventory of their external assets (IP addresses and domains) and internal ones (IP addresses, servers, and domains). As shown in Figure 10, most respondents (77.1%) said that they kept a complete inventory of their assets, while 17.8% said no, and 5.08% did not know. While it is very encouraging to find so many organizations maintaining an asset inventory, it's the accuracy of said inventory that comes into question during a pentest.

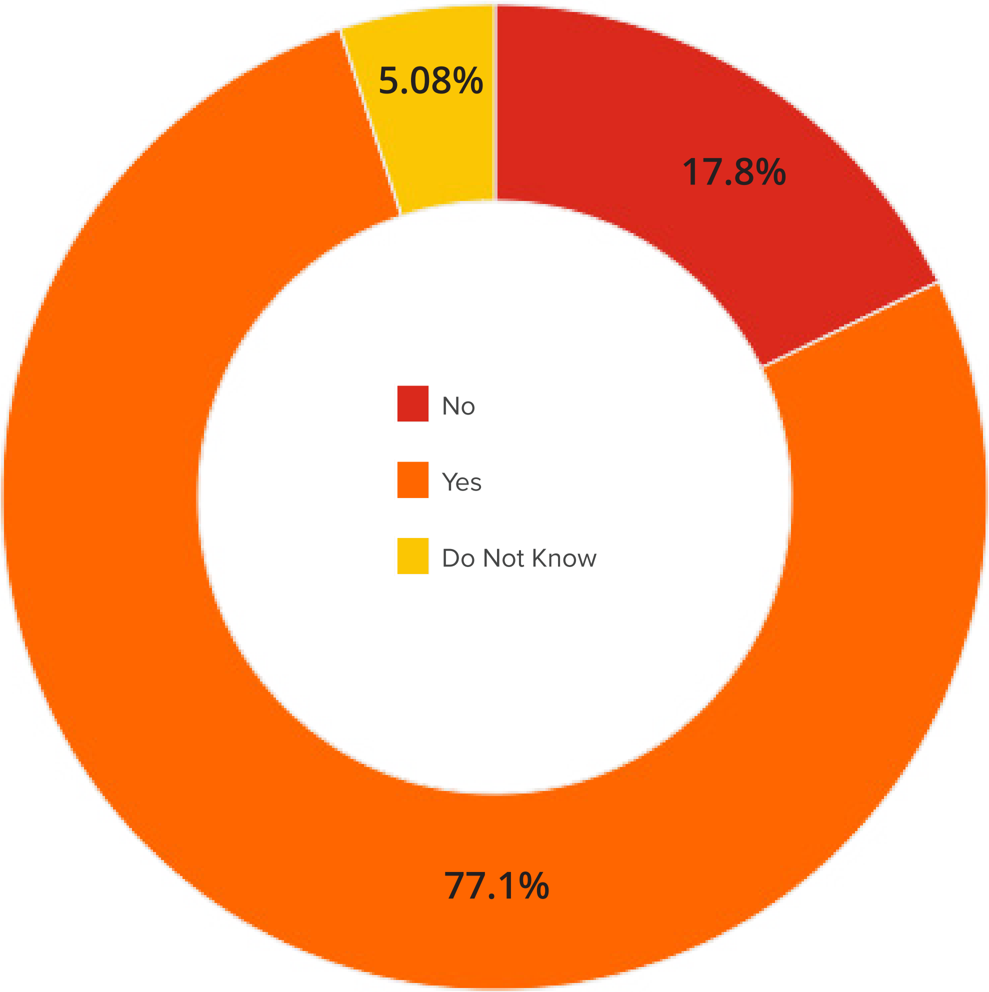


Figure 10 - Asset Inventory

PENETRATION TESTER EXPERIENCE

Overall, GoSecure pentesters mentioned that most companies know their asset inventories. However, the inventory is, most of the time, in an unknown state or not entirely up-to-date. During penetration tests, for example, pentesters have leveraged forgotten and unmaintained servers to enter a company's network. They even mentioned stealing laptops during red team engagements (security tests that allow physical access as well) and most of the time, the employees did not notice that a device was missing.

PRO TIPS ON ASSET INVENTORY

- Ensure that your current IT asset inventory is updated and there is a process to maintain it. The NIST has extensive resources on the topic.
- Consider using offensive security tools to assess your asset inventory. Open source tools like BloodHound (this presentation at DerbyCon explains how to use this tool as a blue team expert) or ADRecon will allow you to have the "attacker's view" of your assets. This can change the IT team's view of assets, while potentially uncover assets that were not in the formal inventory.
- In the long term, establish a comprehensive strategy for the management of assets throughout their life cycle as the basis of other security processes such as risk management, patch management, and disaster recovery.

7 - ENDPOINT VISIBILITY

Endpoint visibility represents visibility on all devices at the edge of a network, such as laptops, desktops, mobiles phones, tablets, etc. We asked how much endpoint visibility respondents have on their entire organization. As shown in Figure 11, we find that 68.4% said high and very high visibility, 23.9% said moderate visibility, and 7.7% said no or low visibility.

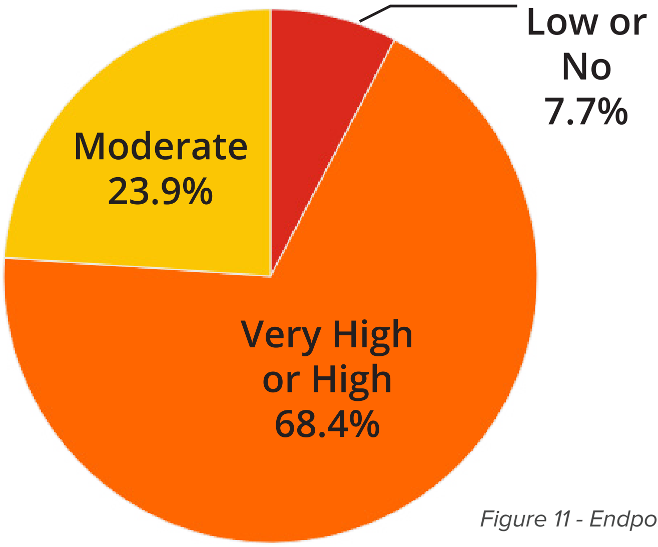


Figure 11 - Endpoint Visibility

PENETRATION TESTING EXPERIENCE

The fact that 68% of the respondents said that they had high endpoint visibility was surprising to penetration testers. They mentioned that the discrepancy may be explained by the idea that endpoint visibility perceived by the respondents is based on more traditional threats instead of more recent techniques using in-memory payloads and weaponized operating system features. However, based on pentesting experience, when compared with the tactics, techniques, and procedures frameworks (TTPs) like the Mitre Att&ck framework, the client's endpoint visibility usually covers only a fraction of the known tactics and techniques.

PRO TIPS ON ENDPOINT VISIBILITY

- Consider an Endpoint Detection and Response (EDR) provider to increase effective endpoint visibility and prevent sophisticated attacks
- Otherwise, tools like Sysmon and Windows Event Forwarding (WEF) / Windows Event Collector (WEC) are free and, when well configured, are a good replacement/complement/addition to an EDR solution

PART 2:
Perceptions Slipups in Cybersecurity

After finding incongruities in the survey results and the penetration testers' experience, we then compared perceived organizational security maturity versus implemented security measures. We selected a question that assessed the respondents' perceived security maturity of their organization and, with a statistical model, examined whether the security measures reported as implemented -or not- in the respondent's organization positively and significantly correlated with such perceived security maturity. Then, we compiled the top 10 vulnerabilities/missing controls found in 65 penetration testing reports. These are presented in The Most Common Attack Vectors subsection along with pro tips for specific new vectors not discussed above. These two analyses uncover potential biases in the defenders' mindset and information gaps that are discussed in the What is Going On? section.

PERCEIVED SECURITY MATURITY CONSIDERING IMPLEMENTED SECURITY MEASURES

The survey started by asking respondents their perception on the overall security maturity of their organization.

"On a scale from 1 to 5, how mature is the information security of your organization?"

As shown in Figure 12, fewer than 4% responded 1, which represents little security maturity, another 20% said 2, a total of 32% said 3, 31% responded 4 and about 13% said 5, which represents high security maturity. **This question allowed us to assess if respondents' perceived security aligned, on average, with the seven measures (from Section 1) that they reported being implemented -or not- in their organization.**

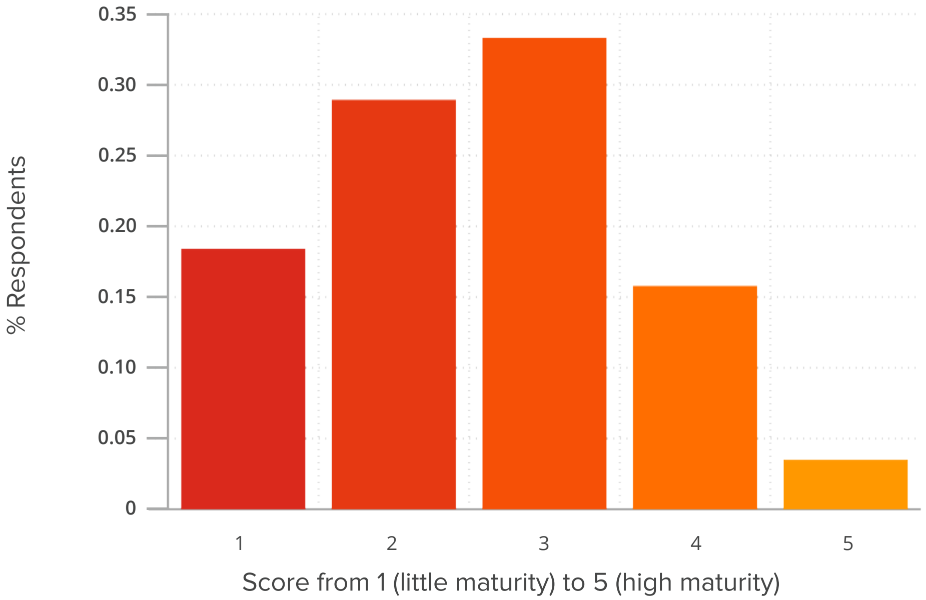


Figure 12 - Respondents' Perception on the Overall Security Maturity of their Organization

To estimate if there exist relationships between respondents' perceived maturity security of their organization and the seven measures mentioned above, we computed a statistical model called an Ordinary Least Square (OLS) regression[1]. For curious readers, the model and the results are explained more thoroughly in the report's Appendix.

The model shows that five security measures reported as implemented significantly and positively correlate with respondents' perception of the security maturity of their organization. The more of these five measures respondents reported as implemented, the higher the perceived security maturity.

- Multi-factor authentication on external assets
- Multi-factor authentication on internal assets
- Timely patch management
- Up-to-date asset inventory
- High endpoint visibility

However, the key takeaways from the model are not the significant relationships, but rather the non-significant ones. Indeed, the model finds that there are no significant relationships between participants' perceived security maturity and two measures:

- Minimum password requirements
- Investigating products for features that could represent a risk

This means that participants' perceived security maturity does not correlate, on average, with whether these security measures are implemented in their organization.

Although the model's results are based on respondents' perceptions (and do not infer anything about actual security measures being implemented), they indicate that there might be potential biases in the defenders' mindset. More precisely, when the results are cross-correlated with penetration testing data presented below, important information gaps in cybersecurity are unraveled.

THE MOST COMMON ATTACK VECTORS

We investigated 65 reports on penetration testing (internal, external, and Web applications) and extracted a total of 182 findings. Table 1 presents the top 10 vulnerabilities and/or missing controls ranked from medium to high in severity, found in the reports. **These ten findings could represent a checklist for any cybersecurity professional wanting to secure the most common attack vectors used by penetration testers. For efficiency purposes, they could be validated and mitigated before purchasing penetration testing services.** This would provide a security baseline and force pentesters to look for alternatives means of entry. Please note that we mixed the different engagement types (internal, external, and Web applications) for the "most common attack vectors" list because the results were interesting. However, we recognize that the presence of NetBIOS/LLMNR and cross-site scripting are two different findings that do not arise from the same context. Future research should focus on a breakdown of the different engagement types. We discuss below the top 10 findings and, if not already discussed above, we offer additional pro tips following each finding.

Table 1 – Most Common Findings from Pentest Reports

Finding	Number of Reports	Percentage in Total
Weak Password Requirements	35	55%
Corporate Services Using Single-Factor Authentication	23	36%
Windows Credentials Stored in Memory	21	33%
Password Reuse	21	33%
Presence of NetBIOS/LLMNR	21	33%
Inadequate Vulnerability Management Process	19	30%
No HTTP Strict Transport Security (HSTS)	17	27%
Domain Controllers or Servers with Internet Access	15	23%
Cross-Site Scripting (XSS)	14	22%
Inadequate Storage of Sensitive Information	14	22%

Weak password requirements, as shown in Table 1, is the most common finding. A weak password is a password that is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack. Such attack uses a subset of all possible passwords, such as words in the dictionary, proper names, words based on the username, or common variations of these themes. This vulnerability is most often the root cause of successful security breaches. For *pro tips* to improve password policy, please refer to section 1.2 above.

Corporate Services Using Single-Factor Authentication is the second most common finding. It represents a security process that requires either something a user knows, something a user has, or something a user "is" to confirm a user's identity. The use of a password is the most popular method for single-factor authentication even though users are known to use weak passwords or reuse them across multiple Websites. Moreover, services relying on passwords can expose the enterprise's network to brute force or password spraying attacks. These attacks are ineffective when multi-factor authentication is enabled. For *pro tips* to implement multi-factor authentication, please refer to section 1.1 above.

Windows credential stored in memory, the third most common finding, is related to several Windows authentication protocols that involve sending the user's password to the target machine. Several of these protocols are enabled by default and store users and service credentials in restricted memory zones, under the protection of the SYSTEM account. That information can be retrieved in clear text using local administrative privileges. We present below two *pro tips* to help prevent credential exfiltration from memory.

PRO TIPS TO PREVENT CREDENTIAL EXFILTRATION FROM MEMORY

- To prevent credentials exfiltration from memory, newer versions of Windows offer a feature called Credential Guard. This feature is extremely efficient at mitigating this vulnerability but requires specific conditions to be put in place.
- An alternative measure is to isolate the process handling authentication in Windows (lsass) with a setting called “RunAsPPL”.

Password reuse is the fourth most common finding and is related to situations where multiple workstations share the same local user and password combination. It is also common to observe domain users sharing the same passwords. To avoid password reuse of local administrator accounts, look at the *pro tip* below.

PRO TIP TO PREVENT PASSWORD REUSE

- Ensure that every single local administrator password account has a different password, this is possible using Microsoft LAPS, a free solution that randomizes local administrator passwords while allowing for easy management.

NetBIOS/LLMNR protocols, now considered obsolete, represent the fifth most common finding. These are typically used in the process of resolving hostnames as multicast but offer no authentication mechanism. This makes them vulnerable to multiple identity theft attacks at the network level. For *pro tips* to mitigate for these legacy protocols, please refer to section 1.5 above.

Inadequate vulnerability management process, the sixth finding, is the cyclical practice of identifying, classifying, and remediating or mitigating vulnerabilities, especially in software and firmware. Vulnerability management programs are considered inadequate when many systems in production are missing security patches or are running on vulnerable software versions. For *pro tips* on patch management, please refer to section 1.4 above.

No HTTP Strict Transport Security (HSTS) is the seventh finding and represents a missing control (rather than a vulnerability per se). It is a security feature implemented in browsers to locally store the digital certificate of visited HTTPS Websites and map them to their respective domain name. Each subsequent visit to a protected Website is redirected automatically to HTTPS and triggers a validation of the certificate presented by the Web server against the one that was previously stored. If the certificates do not match, the browser will restrict access to the Website, as it is detecting ongoing malicious activity. Browsers will only use this feature if a Website sends the HSTS HTTP header. Be aware that correctly handling HSTS requires a well-defined certificate management process to avoid any impact on the users. The *pro tip* below summarizes how to enable HSTS.

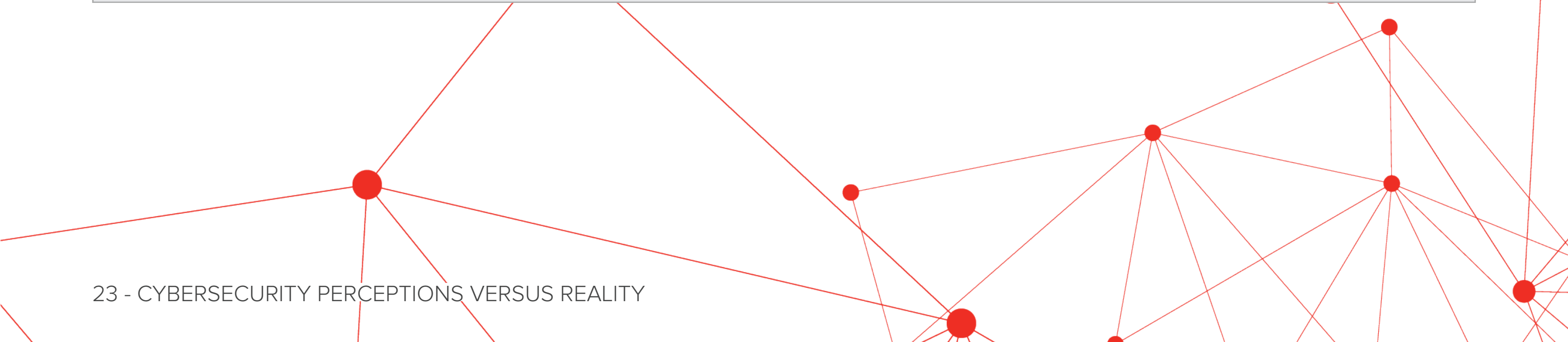
PRO TIP TO ENABLE HSTS

- Enable HSTS by adding a response header with the name ‘Strict-Transport-Security’ and the value ‘max-age=expireTime’, where ‘expireTime’ is the amount of time in seconds that browsers will remember that the site should only be accessed using HTTPS. Consider adding the ‘includeSubDomains’ flag if appropriate.

Domain controllers or servers with Internet represents the eighth most common finding and means that the domain controllers and servers hosted on the corporate network had access to the Internet. Current security standards and best practices advise against this. The *pro tip* below summarizes how this missing control could be mitigated.

PRO TIP TO MITIGATE DOMAIN CONTROLLERS OR SERVERS WITH INTERNET ACCESS

- Restrict access to the Internet for all critical systems in the organization, such as domain controllers and internal servers. If access to the Internet is required to satisfy documented business requirements, the communications should be restricted to the appropriate hosts, services, and ports.



Cross-Site Scripting is the ninth most common finding and a common Web application vulnerability. An application is vulnerable to Cross-Site Scripting (XSS) when user input is reused as-is in the response page. We provide below two *pro tips* to mitigate XSS attacks.

PRO TIPS TO MITIGATE FOR XSS

- Enforce input validation for all user input.
- Using an allow list approach approach with strict regular expressions on expected input is, by far, the most effective strategy to mitigate XSS attacks.

The last most common finding is **inadequate storage of sensitive information** which refers to the methods used to safeguard sensitive information, such as personal information about customers or employees, passwords, banking information, or any information likely to cause harm if known to a malicious individual. Storing this information in plain text in a document, on a workstation, or on a network share is a risky practice. Below are two *pro tips* to mitigate for the storage of cleartext passwords.

PRO TIPS TO MITIGATE FOR STORAGE OF CLEARTEXT PASSWORDS

- No plaintext password files should be tolerated on the network. To prevent this, use a password manager like Keepass or an enterprise-grade password management solution.
- An interesting additional self-diagnostic that can be performed is to scan file shares for password files by searching the term “password” in plain text files (such method is often used by pentesters)

WHAT IS GOING ON?

What is striking from the results presented above is that the two security features that are not associated with respondents' perception of the security maturity of their organization are related to major vectors of attacks found in penetration testing reports. These two security measures are meeting minimum password requirements and product investigation for features vulnerable by default. The major vectors related to them and found in penetration tests are weak password requirements, password reuse, windows credentials stored in memory, and presence of NetBIOS/LLMNR.

Indeed, when minimum password requirements are not met, penetration testers can leverage weak passwords, through attacks like password spraying or brute force, to enter a network. Worse, if multiple workstations share the same credentials, testers may leverage this password reuse to compromise new devices and move through the network undetected.

Moreover, Windows password stored in memory and presence of NetBIOS/LLMNR are two features enabled by default on Windows that represent a vulnerability. These features are exploited by penetration testers all the time. Investigating products for features vulnerable by default should become a priority for information security professionals as even the most robust Firewall cannot mitigate this, leaving the organization at high risk.

Thus, by cross-referencing the results from the ordinary least square regression on perceived security with the top 10 vulnerabilities/missing controls found in 65 penetration testing reports, **we conclude that there is an important information gap in cybersecurity**. Indeed, the main attack vectors found by penetration testers seem to not be perceived as essential elements that contribute to cybersecurity professionals' perception of the security maturity of their organization. There is a need to shift these misaligned perceptions to secure the current weakest links that seem to be found in many organizations.

There is still a lot of work required to secure systems at the technical level. However, this research shows that the challenge is not only technical: there is a need to approach the problem at a higher level, the human one. Understanding the perceptions of cybersecurity professionals led us to recognize that all security measures are not ranked the same way by professionals and that there are still important security measures that are not accounted for.

Future research should consider why this is the case by, for example, interviewing cybersecurity professionals on the matter. There is a need to understand the defenders' decision-making process and how they face this complex task. Factors that influence their thinking process and the potential biases that influence their judgments should be uncovered and discussed. For example, by not investigating products, defenders seem to implicitly trust what they buy, a pattern that reminds the "free-rider problem". Scholars, such as Anderson and Moore (2007)[2], found that information security depends on the sum of all individual efforts and "When it depends on the sum of individual efforts, the burden will tend to be shouldered by the agents with the highest benefit-cost ratio, while the others free-ride" (p.72).

Thus, studying the defenders' decision-making process could help solve the security quandary we are currently in. A human approach would potentially lead to new methods to secure systems, methods that would consider the defenders' perceptions on security, and the difficult task they have at hand.

CONCLUSION

Overall, we find that there is still asymmetrical information between ethical attackers and defenders: the security features that are not found to be related to cybersecurity professionals' sense of security are part of the attack techniques most often used by ethical attackers to break systems. These findings illustrate that, although there are real efforts in the industry to protect systems, there is still a lot of information that is not yet processed and accounted for by defenders. These misaligned perceptions need to be rectified and, by doing so, it is also likely that real attackers would be defeated more often.

This research shows that new perspectives with data cross-referenced can shed light on current trends that are well understood, but still not taken care of. Future research should investigate the human element of cybersecurity: what influences cybersecurity professionals to behave and think the way they do towards the security of their organization.

Authors

Masarah Paquet-Clouston (GoSecure Security Researcher),
Laurent Desaulniers (GoSecure Director of Pentesting Services),
Maxime Nadeau (GoSecure Pentester)

Collaborators

Michael Joyce (Serene-risc Co-Executive Director),
Benoît Dupont (Serene-risc Scientific Director)

Acknowledgments

We thank all participants for taking the time to answer the survey. We also thank Olivier Bilodeau and Alexandre Beaulieu for their valuable comments throughout the writing, as well as Pascal Fortin for helping with the survey and the initial research angle.

ABOUT GOSECURE

APPENDIX

OLS Statistical Model on Perceived Security Maturity and Implemented Security Measures

With the question: “On a scale from 1 to 5, how mature is the information security of your organization?”, we assessed if respondents’ perceived security aligned, on average, with the seven measures that they reported being implemented -or not- in their organization by computing an Ordinary Least Square (OLS) regression. An OLS regression model is a statistical analysis method that estimates the relationship between one or more explanatory variables (known as independent variables) by minimizing the sum of the squares in the difference between the observed and predicted values and an outcome variable (known as the dependent variable). The model formulation is shown in Equation 1.

$$\mathrm{SecMaturity}_i=\beta_0 + \beta_1\mathrm{MFAInternal}_i + \beta_2\mathrm{MFAExternal}_i + \beta_3\ \mathrm{MinPassword}_i +$$

$$\beta_4\ \mathrm{PatchMan}_i + \beta_5\ \mathrm{ProprietaryInv}_i + \beta_{6i}{*}\ \mathrm{AssetInv}_i + \beta_7{*}\ \mathrm{EndPointVis}_i + \varepsilon_i\ (\mathrm{eq.}1)$$

SecMaturity represents the scale at which a respondent i considers the maturity security of his/her organization (from 1, low security, to 5, high security), β_0 is the model’s intercept, MFAInternal represents whether multifactor authentication was reported as implemented at the internal level while MFAExternal is at the external level. MinPassword represents whether the respondent has reported that the minimum password requirements are met in his/her organization, PatchMan represents how long, from a scale from 1 (hours) to 5 (years), it takes for the organization to apply a patch when a new vulnerability is disclosed, according to the respondent. ProprietaryInv indicates whether the respondent has reported that his/her organization investigates a product for specific features representing potential vectors of entry and AssetInv represents whether the respondent has reported that his/her organization is keeping a complete inventory of its assets[3]. Finally, EndPointVis considers whether the respondent has reported having endpoint visibility in his/her organization. Since the descriptive distribution of each explanatory variable has already been presented in Section 1, we do not present them again in this section.

Model Specificities

Lastly, even though the outcome variable (perceived security maturity) is scaled from one to five, as presented in Figure 12, we find that the data fits a linear regression model. As shown in Figure 12, the distribution of the outcome variable follows a normal distribution even though the sampling method imposes discrete values. To confirm that our model followed OLS assumptions, we first computed the Durbin-Watson test and found that there was no autocorrelation in the error terms. Second, we computed the Breush-Pagan test, which showed that there was no heteroscedasticity in the error terms as well. We also computed the variance inflation factors to assess potential multicollinearity problems and all the variance inflation factors (VIFs) were below 1.6, illustrating that there were no multicollinearity issues with the explanatory variables.

Model’s Results

The results of the model are presented in Table 1. The coefficient for each explanatory variable is unstandardized, which means that the coefficient represents a change in the outcome variable (perceived security) when a unit increment is added to the explanatory variable. The standard error (s.e.) estimates the coefficient’s deviation: the smaller it is, the more precise the coefficient is. The p-value determines the significance of the results: a p-value smaller than 0.05 indicates that there exists a relationship between the explanatory variables and the outcome one. We added a column to indicate whether the relationship is significant. Lastly, the R^2 in Table 1 indicates the proportion of variance in the outcome variable that can be explained by the explanatory variables.

Table 1 – Ordinary Least Square Regression Estimating Perceived Security Maturity

	Coeffi-cient	Standard Error (s.e.)	P-Value	Variable Signifi-cant
Intercept (the constant)	1.01	0.49	0.04	yes
Multi-factor authentication – internal	0.24	0.12	0.01	yes
Multi-factor authentication – external	0.31	0.12	0.05	yes
Minimum password require-ments	0.09	0.10	0.40	no
Delay patch management	- 0.15	0.08	0.05	yes
Proprietary product investiga-tion	0.17	0.17	0.31	no
Asset inventory	0.47	0.18	0.01	yes
Endpoint visibility	0.38	0.10	0.00	yes
R^2	0.51			

As shown in Table 1, the intercept and five out of the seven explanatory variables are significant: multi-factor authentication at the internal and external perimeters, patch management, asset inventory, and endpoint visibility.

For multi-factor authentication at the internal perimeter, a one-point increase in reporting to having implemented the feature (from no (0) to partially (1) or from partially (1) to yes (2)) leads to 0.24 (s.e. 0.12) point increase in the respondents’ perceived security maturity. For multi-factor authentication at the external perimeter, a one-point increase in reporting to having implemented the feature (from no (0) to partially (1) or from partially (1) to yes (2)) represents a 0.31 (s.e. 0.12) point increase in perceived security maturity of respondents’ organization. In terms of patch management, a one-point increase in reported delays (a 5-point scale from hours (1) to days (2), or days (2) to weeks (3), or weeks (3) to months (4), or months (4) to years (5)) leads to a 0.15 (s.e. 0.08) point decrease in perceived security maturity. A one-point increase in reporting to have an asset inventory (from no inventory (0) to having one (1)) leads to a 0.47 (s.e. 0.18) point increase in perceived security maturity and finally, a one-point increase in reporting to having endpoint visibility (from 1 to 5, where

1 represents low visibility and 5 high visibility) leads to a 0.38 (s.e. 0.10) point increase in perceived security maturity. The two remaining variables, minimum password requirements and products investigation, are not significant in the model. Thus, whether minimum password requirements are met, and whether products are investigated are both variables that are not associated with respondents' perceived security maturity of their organization.

Lastly, as shown in Table 1, the proportion of variance in the outcome variable that can be explained by the explanatory variables is 38%. This means that there is a certain percentage of the variance in the outcome variable that is explained by other explanatory variables (not included in the model), calling for further investigation on the matter.

[1] - An ordinary least square regression (OLS) model is a statistical analysis method that estimates the relationship between one or more explanatory variables (known as independent variables) and an outcome variable (known as the dependent variable) by minimizing the sum of the squares in the difference between the observed and predicted values.

[2] - Anderson, R., and T. Moore. Information Security Economics And Beyond. In Proceedings of the Annual International Cryptology Conference, 68-91. Springer, Berlin, Germany, 68-91, 2007.

[3] - We recoded as "no" when respondents said that they didn't know if their organization investigated products or kept an updated asset inventory.