Ransomware Control Matrix (RCX)

2023

Industry Analysis of Foundational Controls

www.rcxmatrix.org

Content

I. Introduction 03

II. Executive Summary 04

III. Detailed Results 10

IV. Foundational Control Details 11

V. T1189 - Drive-By Compromise 14

VI. T1190 - Exploit Public-Facing Applications 17

VII. T1133 - External Remote Services 20

VIII. T1566 - Phishing 23

IX. T1195 - Supply Chain Compromise 26

X. T1199 - Trusted Relationships 29

XI. T1078 - Valid Accounts 32

XII. Conclusions and Recommendations 35

XIII. Interesting Observations 36

XIV. Summary 38

XV. References 40

Introduction

As the digital landscape continues to evolve, cybersecurity risks steadily grow in complexity and persistence. Ransomware attacks are no exception to this, often causing catastrophic harm to organizations of all sizes and across all sectors.

The Ransomware Control Matrix (RCX) is a framework designed to help organizations protect against ransomware attacks. It provides a structured approach to identifying and implementing effective controls at different levels of maturity, from foundational, Advanced, and Elite, and includes both detection and mitigation controls. With the RCX, organizations can quickly assess the maturity of deployed security controls, prioritize those controls important to their organization, and create an actionable roadmap for maturing them. Please visit rcxmatrix.org for more indepth information and to access the matrix tool.

The Ransomware Control Matrix serves as a good resource to help create a cybersecurity strategy to mitigate ransomware attacks that use well-known MITRE ATT&CK techniques such as T1189 (Drive-by Compromise), T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1566 (Phishing), T1195 (Supply Chain Compromise), T1199 (Trusted Relationship), and T1078 (Valid Accounts).

Leveraging the Ransomware Control Matrix (RCX) , we undertook a study to shed light on the current state of ransomware preparedness across organizations. This report presents an analysis of the data collected from the online forms completed anonymously by organizations, providing a view of how equipped organizations are in mitigating ransomware threats. By analyzing the extent to which different security measures are being adopted, we aim to provide an overview of the overall preparedness landscape for ransomware attacks.

Our objective with this report is to offer valuable insights that can assist organizations in identifying areas of vulnerability and strength. We believe that this knowledge will enable organizations to strengthen their cybersecurity strategies and improve their defense against ransomware attacks.

The report is structured into three main sections: Executive Summary, Detailed Results, and Recommendations.

We hope that these insights and recommendations will guide your organization in strengthening its resilience against ransomware threats.

Sincerely,

Ed Rojas
Author, Ransomware Control Matrix
www.rcxmatrix.org

Executive Summary

Most/Least Implemented Controls

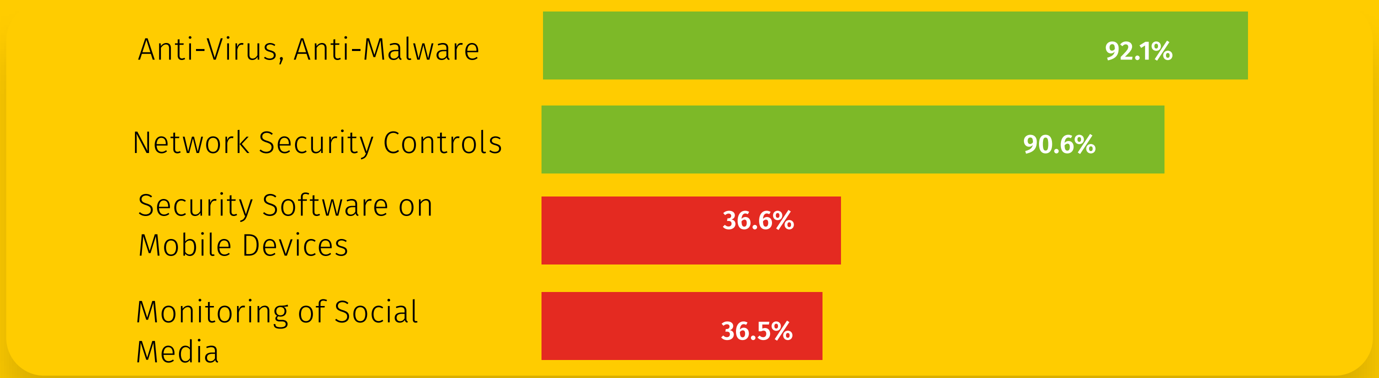

Figure 1 - Most/Least Implemented Controls

This report presents the findings from information provided by **1175 organizations worldwide between April 1st and April 30th, 2023.** The information is focused on controls as identified in the "Foundational category" of the Ransomaware Control Matrix (RCX). Information was collected anonymously and does not identify geographic location, industry type, or organizational size.

The data collected was submitted by a variety of organizations, providing insights into the preparedness of different organizations worldwide to detect and mitigate ransomware attacks.

These findings suggest that many organizations are taking important steps to protect against ransomware attacks, but there is still room for improvement in certain areas. For example, enhancing security measures on mobile devices, monitoring of social media, could greatly enhance organizations' resilience against ransomware threats.

This report provides insights into each cybersecurity countermeasure against MITRE ATT&CK Initial Access Phase techniques and provides recommendations for strengthening cybersecurity controls against ransomware.

These recommendations are aimed at providing a proactive approach to ransomware threats and building a robust and comprehensive cybersecurity posture across organizations.

Companies have adopted basic cybersecurity controls, but there are significant gaps in other areas.

Most Implemented Controls

1. Anti-Virus Anti-Malware (92%)

Most implemented control for T1189 (Drive-by Compromise), T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1566 (Phishing), and T1078 (Valid Accounts). This shows that companies recognize the importance of this basic but critical cybersecurity measure.

2. Network Security Controls (90.6%)

Most implemented control for T1195 (Supply Chain Compromise) showing that most companies understand the importance of network security in mitigating Supply Chain risks.

3. Secure Remote Access (80.9%)

Most implemented control for T1199 (Trusted Relationship), reflecting the fact that companies are aware of the risks associated with remote access and are taking measures to secure it.

Least Implemented Controls

4. Conducting Vendor Risk Assessments (45%)

In the case of T1195 (Supply Chain Compromise), this is the least implemented control. This suggests that many companies may be neglecting an important aspect of supply chain security.

5. Security Software on Mobile Devices (36.6%)

The least implemented control across T1189 (Drive-by Compromise), T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), and T1078 (Valid Accounts). This indicates a significant gap in mobile device security among surveyed companies.

6. Monitoring of Social Media (36.5%)

It's the least implemented control for T1566 (Phishing). This shows that companies need to pay more attention to social media platforms which can often be used for phishing attacks.

MITRE ATT&CK Technique Results

T1189 (Drive-by-Compromise)

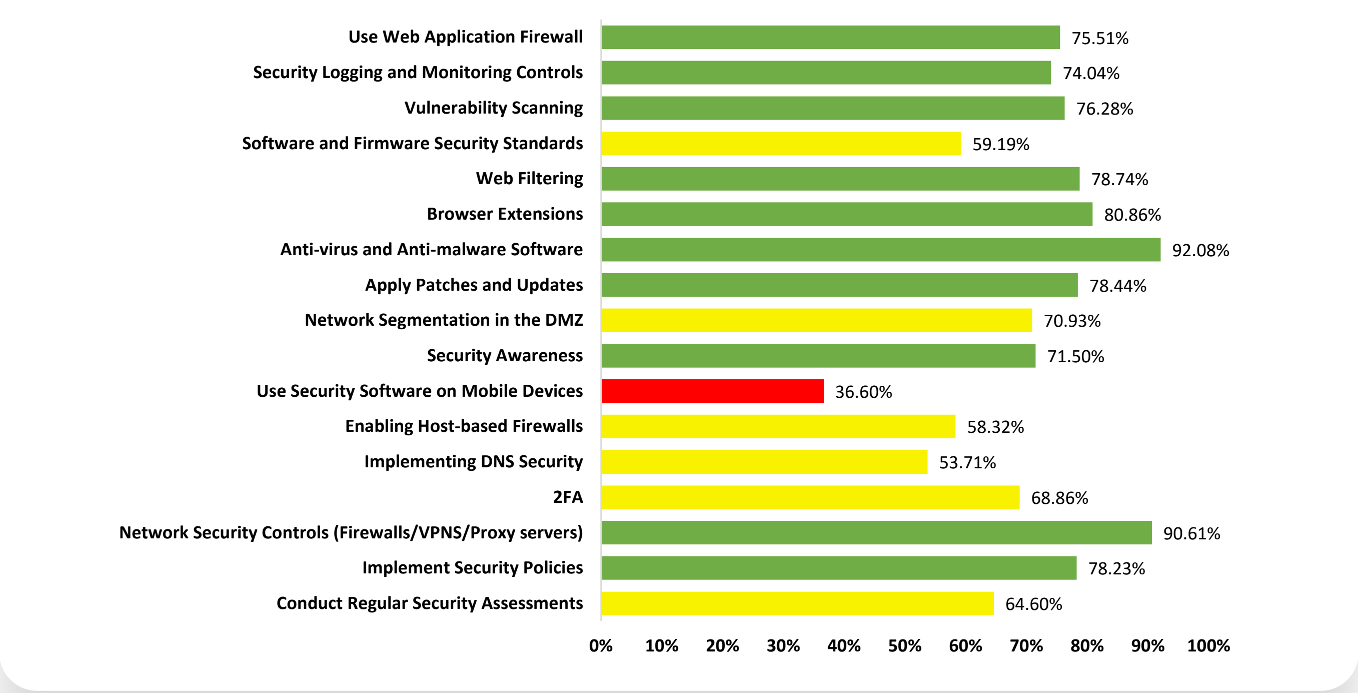

Figure 2 - T1189

T1190 (Exploit Public-Facing Applications)

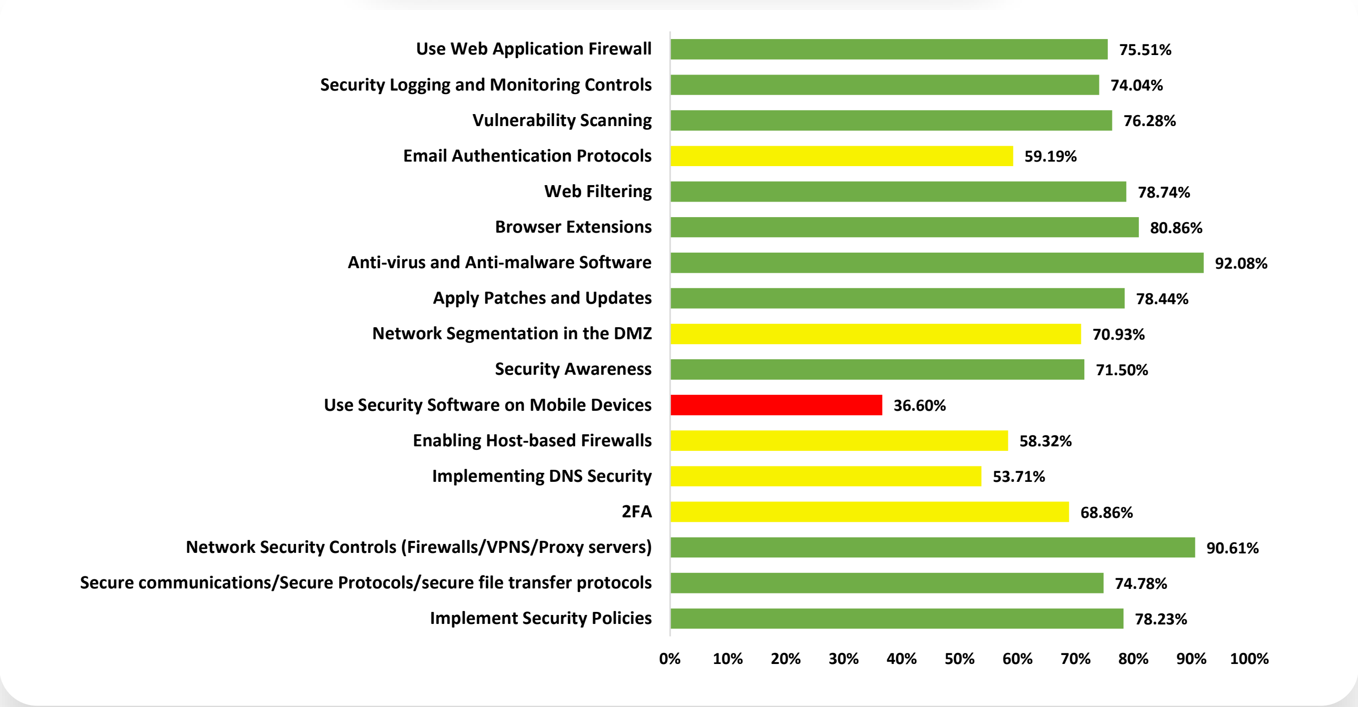

Figure 3 - T1190

MITRE ATT&CK Technique Results

T1133 (External Remote Systems)

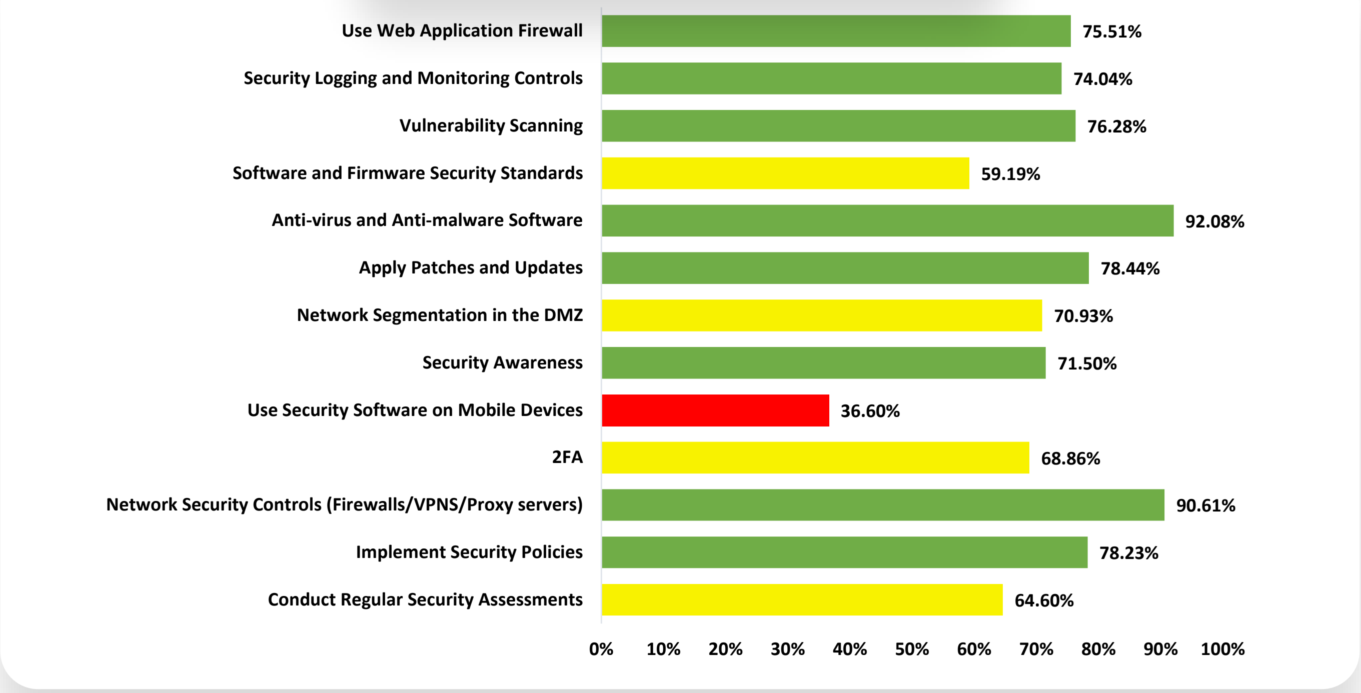

Figure 4 - T1133

T1566 (Phishing)

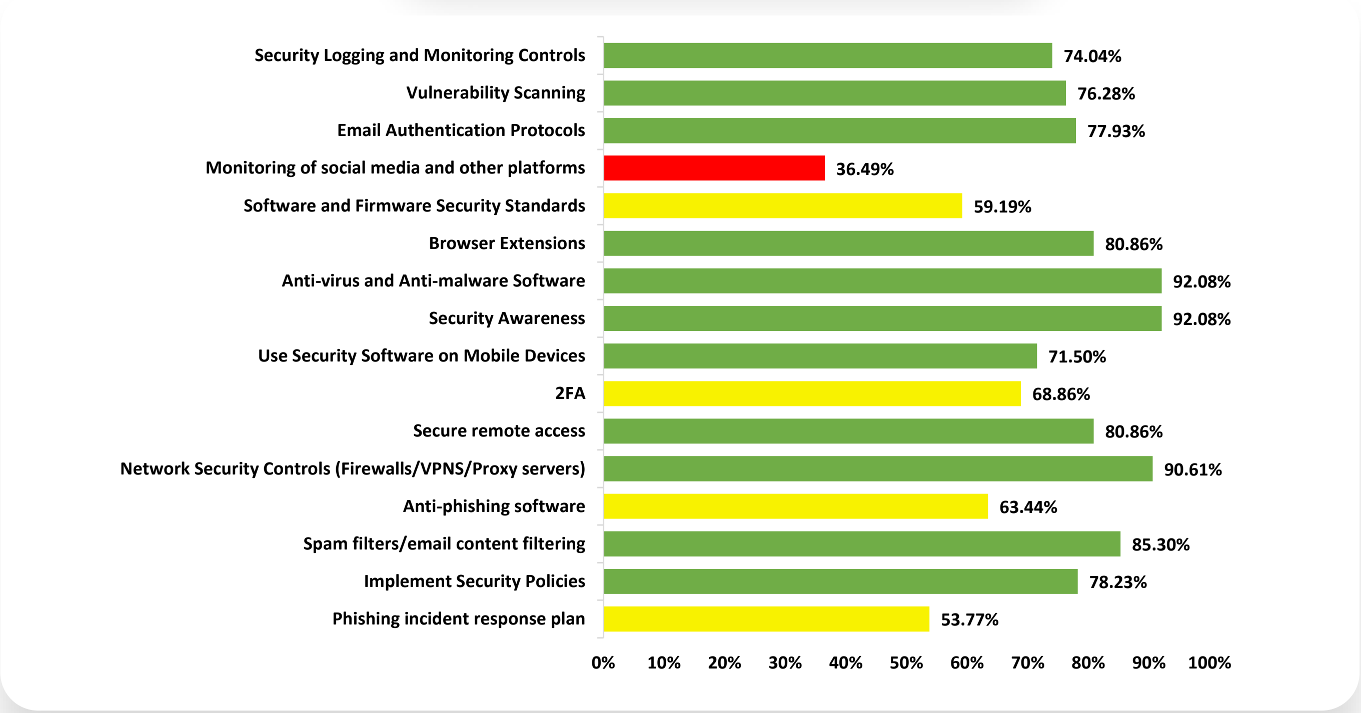

Figure 5 - T1566

MITRE ATT&CK Technique Results

T1195 (Supply Chain Compromise)

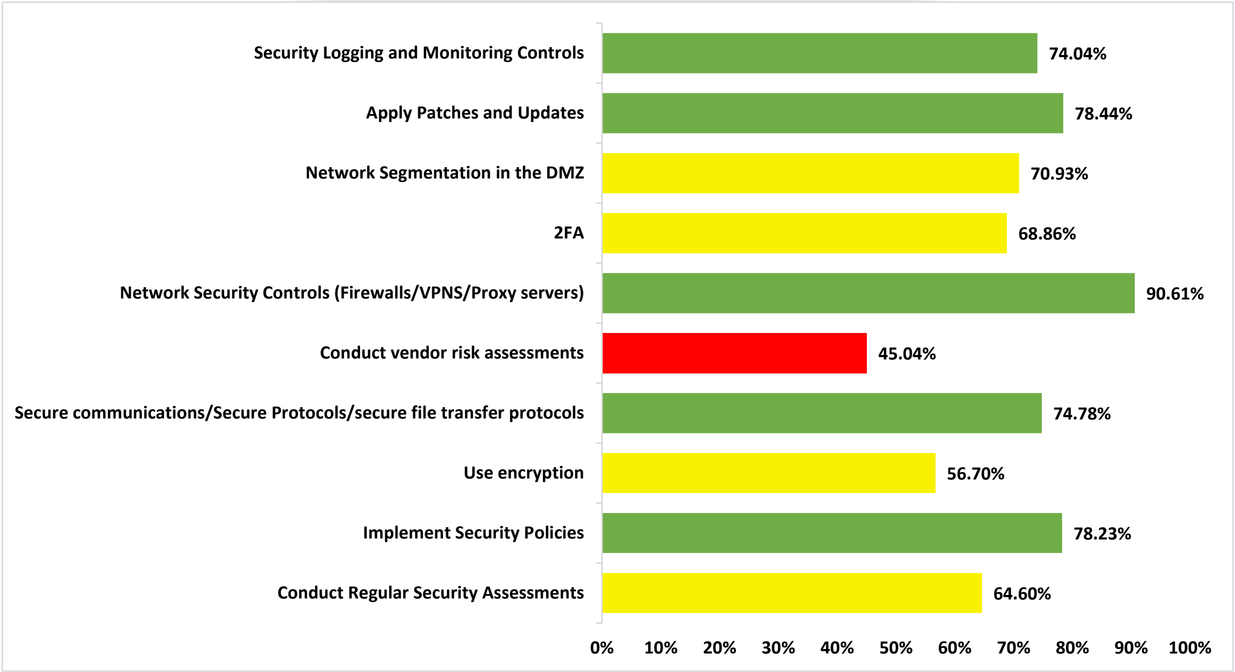

Figure 6 - T1195

T1199 (Trusted Relationships)

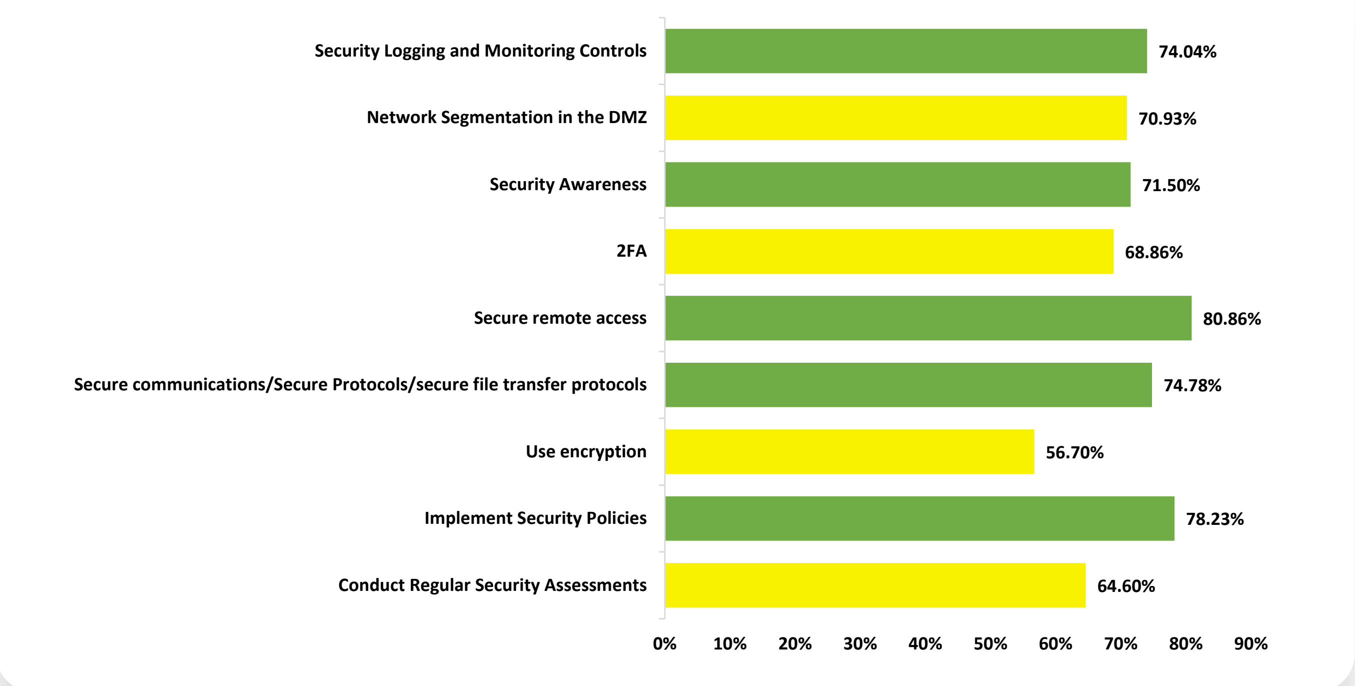

Figure 7 - T1199

MITRE ATT&CK Technique Results

T1078 (Valid Accounts)

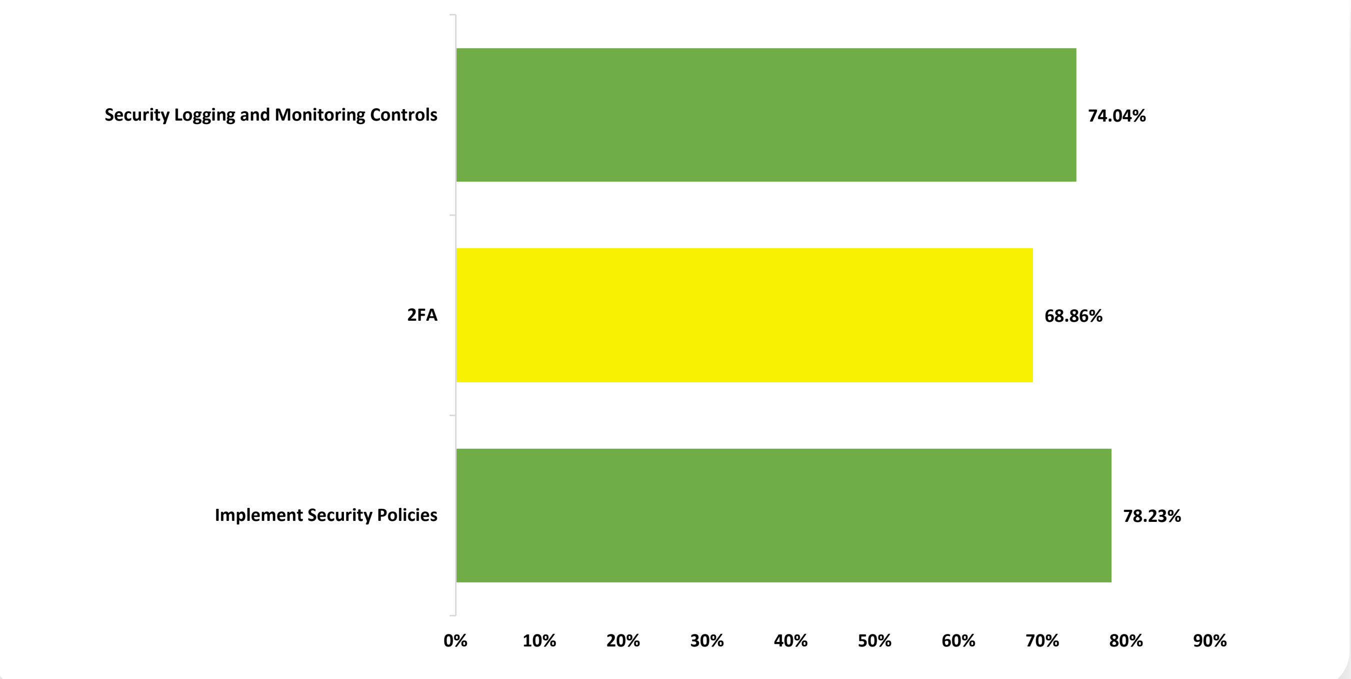

Figure 8 - T1078

Detailed Results

The detailed results section offers a detailed analysis of the data gathered via the Ransomware Control Matrix online forms.

This section provides a detailed view of the level of preparedness and implementation of security controls amongst different organizations in the face of various ransomware techniques.

Current Maturity represents the controls deployed for each MITRE ATT&K Technique, and Residual risk represents the inherent risk remaining for that specific technique. For example, an organization that has 8 of the 13 identified controls installed, has a 62% maturity and a 38% residual risk.

Current Maturity/Residual Risk

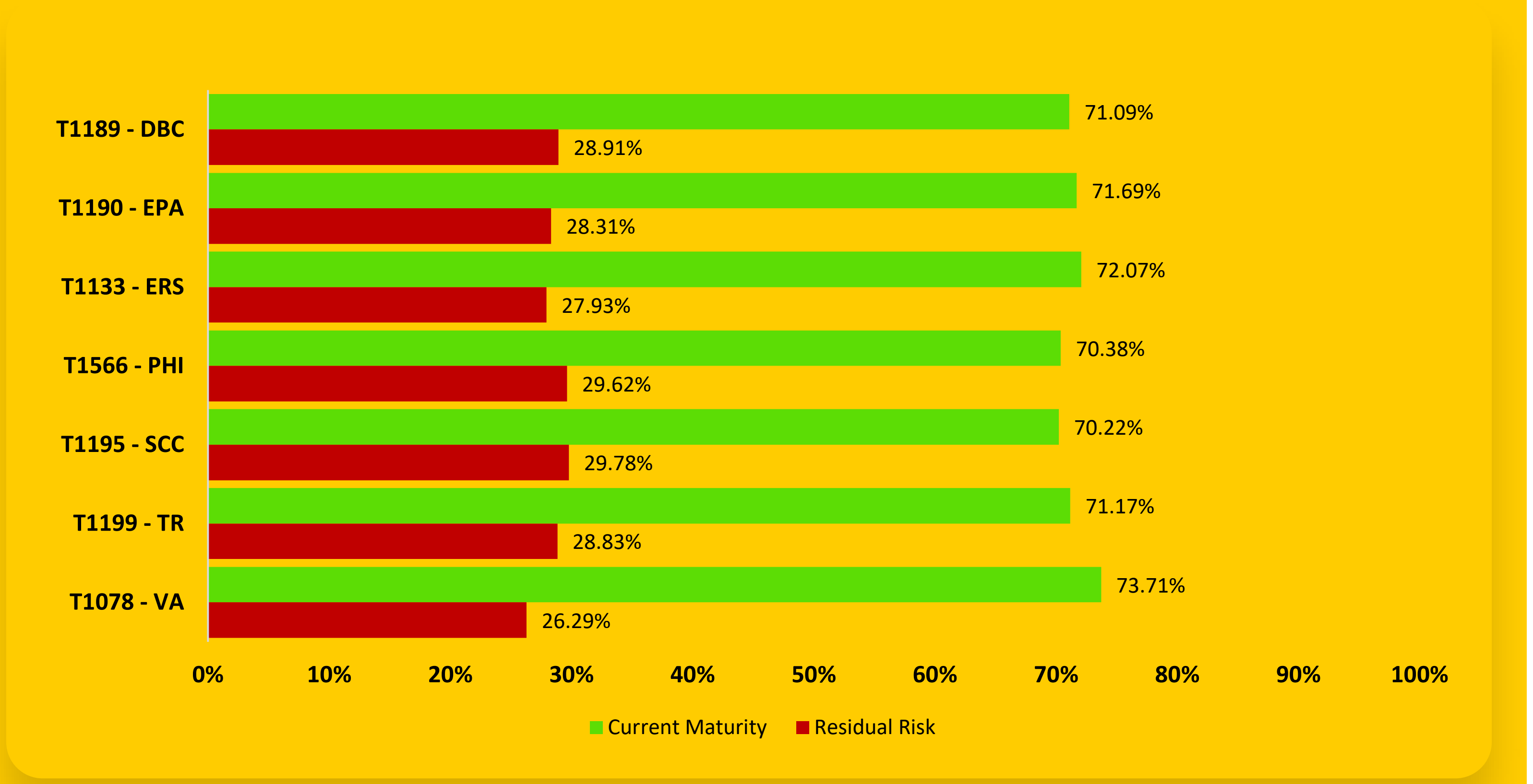

Figure 9 - Current Maturity/Residual Risk

Foundational Controls

The following three pages provide detailed information for each of the 26 controls identified as Foundational Controls.

01

Use Web Application Firewall (75.5%)

Using a web application firewall is important to prevent adversaries from exploiting public-facing applications, such as websites, databases, or services, to gain initial access to a network. The data collected shows that 75.5% of organizations have this control installed, but some organizations are still exposed to potential exploitation.

02

Security Logging and Monitoring Controls (74%)

Security logging and monitoring controls are essential to detect, respond, and prevent ransomware attacks. The data collected shows that 74% of organizations have these controls installed, but there is still room for improvement to detect ransomware attacks.

03

Vulnerability Scanning (76.3%)

Vulnerability scanning is important to protect systems and software from ransomware attacks. The data collected shows that 76.3% of organizations have this control installed, but some organizations are still at risk of being compromised.

04

Email Authentication Protocols (77.9%)

Email authentication protocols are important to protect against email-based cyber threats such as phishing or spear phishing emails and other cyber threats. The data collected shows that 77.9% of organizations have email authentication protocols installed, but some organizations are at risk of being compromised by email-based threats.

05

Monitoring of Social Media (36.5%)

Monitoring of social media and other platforms is important to protect organizations against social media-based threats such as phishing or spear phishing emails and other cyber threats. The data collected shows that 36.5% of organizations have monitoring of social media and other platforms control installed, but some organizations are at risk of being compromised by social media-based attacks.

06

Software and Firmware Security Standards (59.2%)

Software and firmware security standards are important to ensure the integrity, authenticity, and resiliency of software and firmware products against ransomware attacks that can corrupt or encrypt them. The data collected shows that 59.2% of organizations have this control installed, but some organizations are still using insecure or outdated software and firmware.

07

Web Filtering (78.7%)

Web filtering is important to block malicious web requests and content that could lead to a drive-by compromise of systems. The data collected shows that 78.7% of organizations have this control installed, but some organizations are still susceptible to web-based attacks.

08

Browser Extensions (80.9%)

Browser extensions are small programs that add new features or customize the appearance or function of your web browser. The data collected shows that 80.9% of organizations have this control installed, but some organizations are still using unapproved or malicious extensions that could compromise their security or privacy.

09 Anti-virus and Anti-Malware Software (92%)

Anti-virus and anti-malware software are important to detect and remove ransomware and other types of malware that can infect your systems and encrypt your data. The data collected shows that 92% of organizations have this control installed, but some organizations are still unprotected or outdated.

10 Apply Patches and Updates (78.4%)

Applying patches and updates is important to fix security flaws and weaknesses in systems and software that could be exploited by ransomware attacks. The data collected shows that 78.4% of organizations have this control installed, but some organizations are still using outdated or vulnerable versions.

11 Network Segmentation in the DMZ (70.9%)

Network segmentation in the DMZ is important to isolate and protect services and resources that are exposed to the Internet from the internal network of an organization. The data collected shows that 70.9% of organizations have this control installed, but some organizations are still connected to a flat or unsegmented network.

12 Security Awareness (71.5%)

Security awareness is important to educate and empower employees to protect the organization’s data and systems from ransomware and other cyberattacks. The data collected shows that 71.5% of organizations have this control installed, but some organizations are still lacking security training or awareness programs.

13 Use Security Software on Mobile Devices (36.6%)

Using security software on mobile devices is important to protect them from malware, phishing, and other cyberattacks that could compromise their data or access to the network. The data collected shows that 36.6% of organizations have this control installed, but the majority of organizations are still vulnerable.

14 Enabling Host-based Firewalls (58.3%)

Enabling host-based firewalls is important to filter and block unauthorized network traffic flowing into or out of the device. The data collected shows that 58.3% of organizations have this control installed, but large number of organizations are still unprotected or misconfigured.

15 Implementing DNS Security (53.7%)

Implementing DNS security is important to protect DNS infrastructure and data from cyberattacks that could compromise their integrity, availability, or confidentiality. The data collected shows that 53.7% of organizations have this control installed, but the majority of the organizations are still using insecure or unencrypted DNS protocols.

16 Two-Factor Authentication (2FA) (68.9%)

2FA is important to verify users’ identities through two different authentication factors, such as a password and a code sent to their phone or email. The data collected shows that 68.9% of organizations have this control installed, but some organizations are still using only one authentication factor.

17 Secure Remote Access (80.9%)

Secure remote access is important to protect against remote-based cyber threats such as unauthorized access or data breaches. The data collected shows that 80.9% of organizations have secure remote access control installed, but some organizations are at risk of being compromised by threats such as Remote Access Trojans (RATs), Distributed Denial of Service (DDoS) attacks, spying and blackmail attempts, cryptomining.

18 Network Security Controls (90.6%)

Network security controls are used to protect the network infrastructure and data from unauthorized access, misuse, or theft. The data collected shows that 90.6% of organizations have this control installed, but some organizations are still lacking adequate security measures such as firewalls, VPNs, or proxy servers.

19 Anti-Phishing Software (63.4%)

Anti-phishing software is important to protect against phishing attacks which can lead to unauthorized access or data breaches. The data collected shows that 63.4% organizations have anti-phishing software installed, but some organizations are exposed to threats that include RATs, DDoS), spying and blackmail attempts, and cryptomining.

20 Spam Filters/Email Content Filtering (85.3%)

Spam filters/email content filtering is important to protect against phishing attacks and other email-based cyber threats. The data collected shows that 85.3% of organizations have spam filters/email content filtering installed,but some organizations are at risk of being exposed to phishing attacks and other email-based threats.

21 Conduct Vendor Risk Assessments (45%)

Vendor risk assessments are important as they help organizations identify and mitigate risks associated with third-party vendors and can take steps to mitigate those risks. The data collected shows that 45% of organizations have this control installed, but some organizations are vulnerable to attacks that target third-party vendors as a way to gain access to an organization’s network.

22 Secure Communications/Secure Protocols/Secure File Transfer Protocols (74.8%)

Secure communications such as secure file transfer protocols are important to protect your data from unauthorized access, misuse, or theft. The data collected shows that 74.8% of organizations have this control installed, but some organizations don’t employ secure communications protocols may be at risk of data breaches.

23 Use encryption (56.7%)

Encryption can help protect against ransomware by making it harder for cybercriminals to intercept your data. They would need to break into your system first, then crack your encryption algorithm, which makes you a less appealing target. The data collected shows that 56.7% of organizations have this control installed, but some organizations don’t employ encryption putting them at risk of stolen credentials, internal threats, and data breaches.

24 Implement security policies (78.2%)

Implementing security policies is important to define and enforce rules, expectations, and approach to maintain the confidentiality, integrity, and availability of its data. The data collected shows that 78.2% of organizations have this control installed, but some organizations are still lacking clear or consistent security policies.

25 Conduct Regular Security Assessments (64.6%)

Conducting regular security assessments is important to identify and address security risks and vulnerabilities in the organization’s systems, data, and processes. The data collected shows that 64.6% of organizations have this control installed, but some systems are still untested or outdated.

26 Phishing Incident Response Plan (53.8%)

Having a phishing incident response plan is important to protect against phishing attacks and other email-based cyber threats. The data collected shows that 53.8% of organizations have a phishing incident response plan, but some organizations are at risk of being exposed to phishing attacks and other email-based threats

T1189 Drive-by Compromise

A Drive-by Compromise, labeled as T1189 in the MITRE ATT&CK framework, is a cyber-attack technique where a victim's device gets infected by malware simply by visiting a website. In this attack method, the attacker identifies a vulnerability either in the victim's browser or in the software that's being run by the browser, such as a plug-in or an extension.

An attacker compromises a legitimate website (or creates a malicious website) and injects it with malicious code. When a user visits this compromised website, the malicious code on the site exploits vulnerabilities in the user's web browser or the browser's plugins. It then automatically downloads and installs malware onto the user's system without their knowledge or interaction - hence the term “drive-by”.

This technique can have wide-reaching impacts as it doesn't require any user interaction beyond visiting the compromised site. Even cautious users can become victims. Implementing effective controls against this technique is very important. Such controls may include keeping software and web browsers updated to the latest versions, employing strong anti-virus and anti-malware solutions, using web filters, and training users about the risks of visiting untrusted websites.

CONTROL	INSTALLED	NOT INSTALLED	NEED INFORMATION	T1189 - DBC
1. Use Web Application Firewall	885	275	12	75.5%
2. Security Logging and Monitoring Controls	807	249	34	74%
3. Vulnerability Scanning	804	228	22	76.3%
4. Software and Firmware Security Standards	573	315	80	59.2%
5. Web Filtering	774	188	21	78.7%
6. Browser Extensions	748	145	32	80.9%
7. Anti-virus and Anti-malware Software	883	66	10	92.1%
8. Apply Patches and Updates	746	162	43	78.4%
9. Network Segmentation in the DMZ	671	245	30	70.9%
10. Security Awareness	675	229	40	71.5%
11. Use Security Software on Mobile Devices	340	537	52	36.6%
12. Enabling Host-based Firewalls	540	341	45	58.3%
13. Implementing DNS Security	499	377	53	53.7%
14. 2FA	648	260	33	68.9%
15. Network Security Controls	849	80	8	90.6%
16. Implement Security Policies	726	161	41	78.2%
17. Conduct Regular Security Assessments	604	296	35	64.6%

T1189 Drive-By Compromise

> One of the most encouraging aspects of the survey is the high implementation rate of Anti-virus and Anti-malware Software, as well as Network Security Controls such as Firewalls, VPNs, and Proxy servers. These security measures are foundational and play a critical role in protecting against a multitude of cyber threats, including T1189.

Significance of results

The survey results highlight some critical aspects of the industry's preparedness to deal with T1189 - Drive-by Compromise. The data suggests varying degrees of readiness, with some areas of security receiving more focus than others.

One of the most encouraging aspects of the survey is the high implementation rate of Anti-virus and Anti-malware Software, as well as Network Security Controls such as Firewalls, VPNs, and Proxy servers. These security measures are foundational and play a critical role in protecting against a multitude of cyber threats, including T1189.

Web Application Firewalls, Security Logging and Monitoring Controls, Vulnerability Scanning, Web Filtering, and applying Patches and Updates also saw robust adoption, highlighting that most respondents are taking necessary precautions to secure their environments.

Some areas of concern are the relatively low adoption rate of security measures like using Security Software on Mobile Devices, enabling Host-based Firewalls, and implementing DNS security. This suggests potential vulnerabilities in the industry. Mobile devices can often be an easy entry point for cybercriminals if not properly secured. Host-based Firewalls and DNS security measures are crucial in safeguarding individual systems and protecting Internet communications.

The relatively low implementation rate of Software and Firmware Security Standards indicates potential weak spots in the defense against T1189. Since this tactic often exploits vulnerabilities in software or firmware, having rigorous security standards for these components is essential.

Even though Two-factor authentication (2FA) is not the least implemented control, its adoption rate of just under 70% suggests that there is room for significant improvement. We will need to review controls in the “Advanced level” as these include MFA as well as IAM, that are more advanced controls than 2FA, to provide us with a clearer view regarding identification controls.

What is interesting is a substantial number of respondents indicated the need for more information across multiple controls. This could imply that awareness and understanding of these controls may be lacking for some, emphasizing the need for increased industry-wide education and training or an improvement on internal continuous assessment process of the cybersecurity program.

Conclusions

71.1%

This data shows a range of implementation rates for different controls related to T1189, with the highest rates for Anti-virus and Anti-malware Software and Network Security Controls, and the lowest rates for Using Security Software on Mobile Devices.

The survey results highlight some critical aspects of the industry‘s preparedness to deal with T1189 - Drive-by Compromise. The data suggests varying degrees of readiness, with some areas of security receiving more focus than others.

There are strong areas of preparedness for T1189 in the industry. The data collected reveals certain vulnerabilities and gaps that need to be addressed to ensure comprehensive defense against such threats. It also highlights the need for continuous education and information sharing among industry participants.

T1189 - Drive-By Compromise Detail

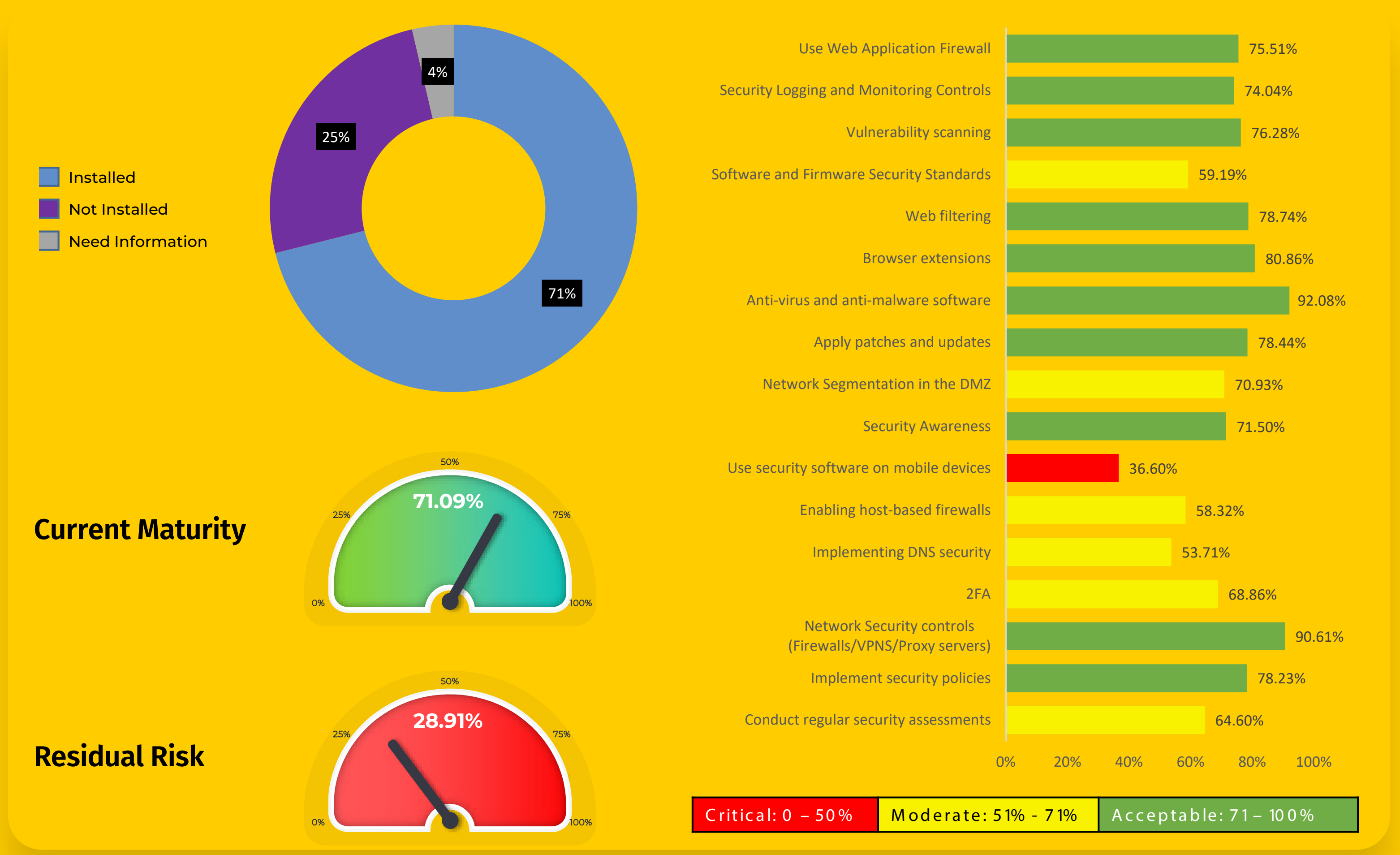

Figure 10 - T1189 - Drive-By Compromise Detail

T1190 Exploit Public-Facing Applications

This tactic involves exploiting software vulnerabilities in public-facing applications to gain unauthorized access to a system or network. Public-facing applications are those that are accessible over the Internet and often include web servers, Content Management Systems (CMS), customer databases, and other similar resources. These can be vulnerable to various forms of exploitation, such as SQL injection, Cross-Site Scripting (XSS), Remote File Inclusion (RFI), or exploiting known software vulnerabilities that have not yet been patched by the user. Once a vulnerability is exploited successfully, the attacker can often run arbitrary code, manipulate the application, gain access to the underlying system, or even establish a foothold for further internal exploitation.

Organizations can safeguard against T1190 attacks by regularly updating and patching software, employing security measures like Web Application Firewalls (WAFs), monitoring system logs for suspicious activity, and performing regular security audits of their public-facing applications.

CONTROL	INSTALLED	NOT INSTALLED	NEED INFORMATION	T1189 - DBC
1. Use Web Application Firewall	885	275	12	75.5%
2. *Security Logging and Monitoring Controls*	807	249	34	74%
3. *Vulnerability Scanning*	804	228	22	76.3%
4. *Software and Firmware Security Standards*	573	315	80	59.2%
5. *Web Filtering*	774	188	21	78.7%
6. *Browser Extensions*	748	145	32	80.9%
7. *Anti-virus and Anti-malware Software*	883	66	10	92.1%
8. *Apply Patches and Updates*	746	162	43	78.4%
9. *Network Segmentation in the DMZ*	671	245	30	70.9%
10. *Security Awareness*	675	229	40	71.5%
11. *Use Security Software on Mobile Devices*	340	537	52	36.6%
12. *Enabling Host-based Firewalls*	540	341	45	58.3%
13. *Implementing DNS Security*	499	377	53	53.7%
14. *2FA*	648	260	33	68.9%
15. *Network Security Controls*	849	80	8	90.6%
16. *Secure communications/Secure Protocols...*	694	190	44	74.8%
17. *Implement Security Policies*	726	161	41	78.2%

T1190 Exploit Public-Facing Applications

The results for Tactic T1190 - Exploit Public-Facing Application reveal a mixed picture of the industry‘s preparedness. The implementation rates of certain control measures are highly encouraging, while others indicate potential areas of weakness that could be exploited.

Significance of results

The high adoption rates of Anti-virus and Anti-malware Software, Network Security Controls, and the use of a web Application Firewall are all positive signs. These are fundamental security measures that form the first line of defense against most threat vectors, including the exploitation of public-facing applications.

The wide adoption of Browser Extensions, Vulnerability Scanning, and the Application of Patches and Updates indicate a strong understanding of the threat landscape and the measures needed to counter it. The Implementation of Secure Communication Protocols also reflects a heightened focus on data integrity and privacy.

There are areas where the industry could improve. The lower implementation rates of Security Software on Mobile Devices, DNS security, and Host-based Firewalls suggest possible gaps in the defensive posture of many organizations. These areas represent potential avenues of attack that could be exploited by adversaries, particularly as mobile devices and DNS-based attacks become increasingly common.

The moderate implementation rates of Software and Firmware Security Standards and security awareness training suggest that there could be a lack of standardized security practices across the industry, as well as potential gaps in employee understanding of security best practices. This could be addressed through wider adoption of industry security standards and increased investment in security awareness training.

The industry‘s overall preparedness for T1190 - Exploit Public-Facing Application is quite good, but the lower adoption rates for certain security measures highlight areas that require additional focus. By addressing these gaps, organizations can further strengthen their defenses against the exploitation of public-facing applications.

Conclusions

71.7%

Results indicate a strong adoption of various control measures to mitigate the risk of T1190. There is a noticeable lack of mobile device security and DNS security, which could potentially be areas for improvement. A more universal adoption of Software and Firmware Security Standards, as well as Host-based Firewalls, could bolster defenses against T1190 exploits.

These findings underscore the need for a more balanced and comprehensive approach for security measures that address potential points of vulnerability. The most implemented controls represent fundamental and critical aspects of cyber security, the least implemented ones could expose organizations to unnecessary risks if not addressed promptly.

T1190 - Exploit Public-Facing Applications

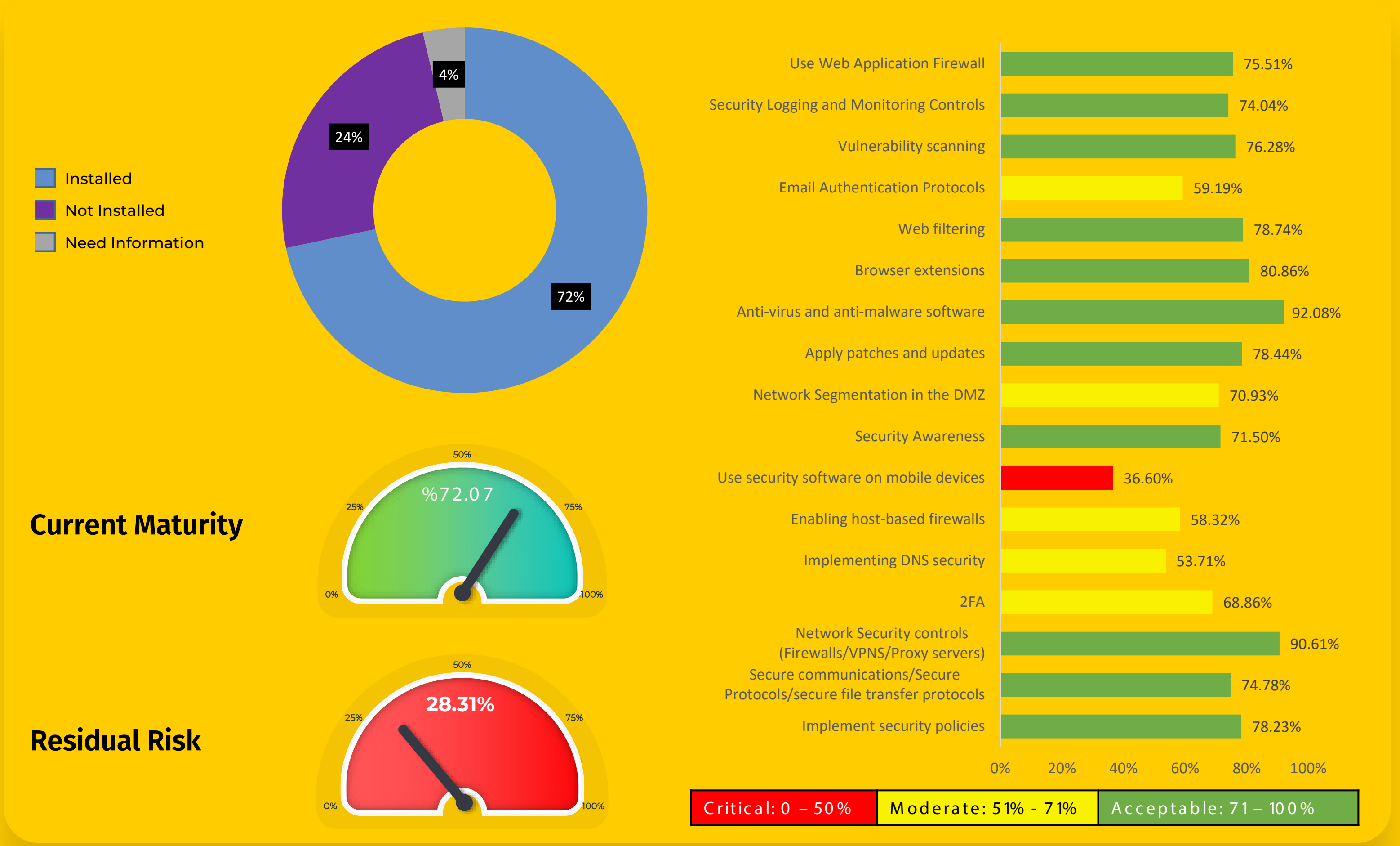

Figure 11 - T1190 - Exploit Public-Facing Applications Detail

T1133 External Remote Services

Involves the use of remote services that are accessible from outside the organization. These remote services include virtual private network (VPN) connections, remote desktop services, or any other type of remote network service that allows users to connect from external networks. External remote services are crucial for business operations, especially in today's digital world where remote work and global collaboration are common. These services allow authorized personnel to access internal resources from any location, enhancing operational flexibility and productivity.

These services represent a significant attack surface for threat actors. If not properly secured, they can be exploited to gain unauthorized access to an organization's network, often bypassing perimeter defenses. Attackers can then carry out further malicious activities, including data theft, network disruptions, or even ransomware attacks.

It is important to ensure that these services are properly configured and secured. This involves implementing strong authentication methods (like multi-factor authentication), regular patching and updating of the remote service software, and rigorous monitoring and logging to detect any abnormal activities.

CONTROL	INSTALLED	NOT INSTALLED	NEED INFORMATION	T1189 - DBC
1. Use Web Application Firewall	885	275	12	75.5%
2. *Security Logging and Monitoring Controls*	807	249	34	74%
3. *Vulnerability Scanning*	804	228	22	76.3%
4. *Software and Firmware Security Standards*	573	315	80	59.2%
5. *Anti-virus and Anti-malware Software*	883	66	10	92.1%
6. *Apply Patches and Updates*	746	162	43	78.4%
7. *Network Segmentation in the DMZ*	671	245	30	70.9%
8. *Security Awareness*	675	229	40	71.5%
9. *Use Security Software on Mobile Devices*	340	537	52	36.6%
10. *Network Security Controls*	849	80	8	90.6%
11. *Implement Security Policies*	726	161	41	78.2%
12. *Conduct Regular Security Assessments*	604	296	35	64.6%

T1133 External Remote Services

The data indicates that more work needs to be done to improve preparedness for T1133 (External Remote Services). There should be a greater focus on enhancing security on mobile devices, improving software and firmware security standards, and increasing the frequency of security assessments. By addressing these gaps, organizations can further strengthen their defenses against threats associated with external remote services.

Significance of results

One notable finding is the high implementation rates of certain controls. Anti-virus and Anti-malware Software, with a rate of 92.1%, and Network Security Controls, at 90.61%, demonstrate that organizations recognize the significance of these fundamental security measures in safeguarding against external remote service threats.

Moderate implementation rates were observed for controls such as Security Logging and Monitoring Controls, Use of Web Application Firewall, and Application of Patches and Updates, ranging between 74% and 78%. A significant number of organizations have adopted these measures, but there is room for greater implementation to further strengthen defenses against external remote services.

Some controls showed lower rates of implementation. For instance, the Use of Security Software on Mobile Devices had an implementation rate of only 36.6%. Organizations may be underestimating the risks associated with mobile devices, leaving them vulnerable to external remote service threats.

The implementation rate for Software and Firmware Security Standards stood at 59.2%, indicating the need for organizations to prioritize regular updates and patches to mitigate potential vulnerabilities.

One area that requires improvement is conducting regular security assessments. With a rate of 64.6%, organizations need to be more proactive in identifying and addressing security gaps and vulnerabilities in their systems related to external remote services.

Conclusions

71.7%

The survey highlights the areas where organizations are well-prepared and identifies gaps where more focus is needed to safeguard against the threat associated with T1133 - External Remote Services.

These results indicate a need for increased focus and resources on enhancing security on mobile devices and improving software and firmware security standards. Organizations should prioritize these areas to better protect against threats associated with external remote services.

T1133 - External Remote Services

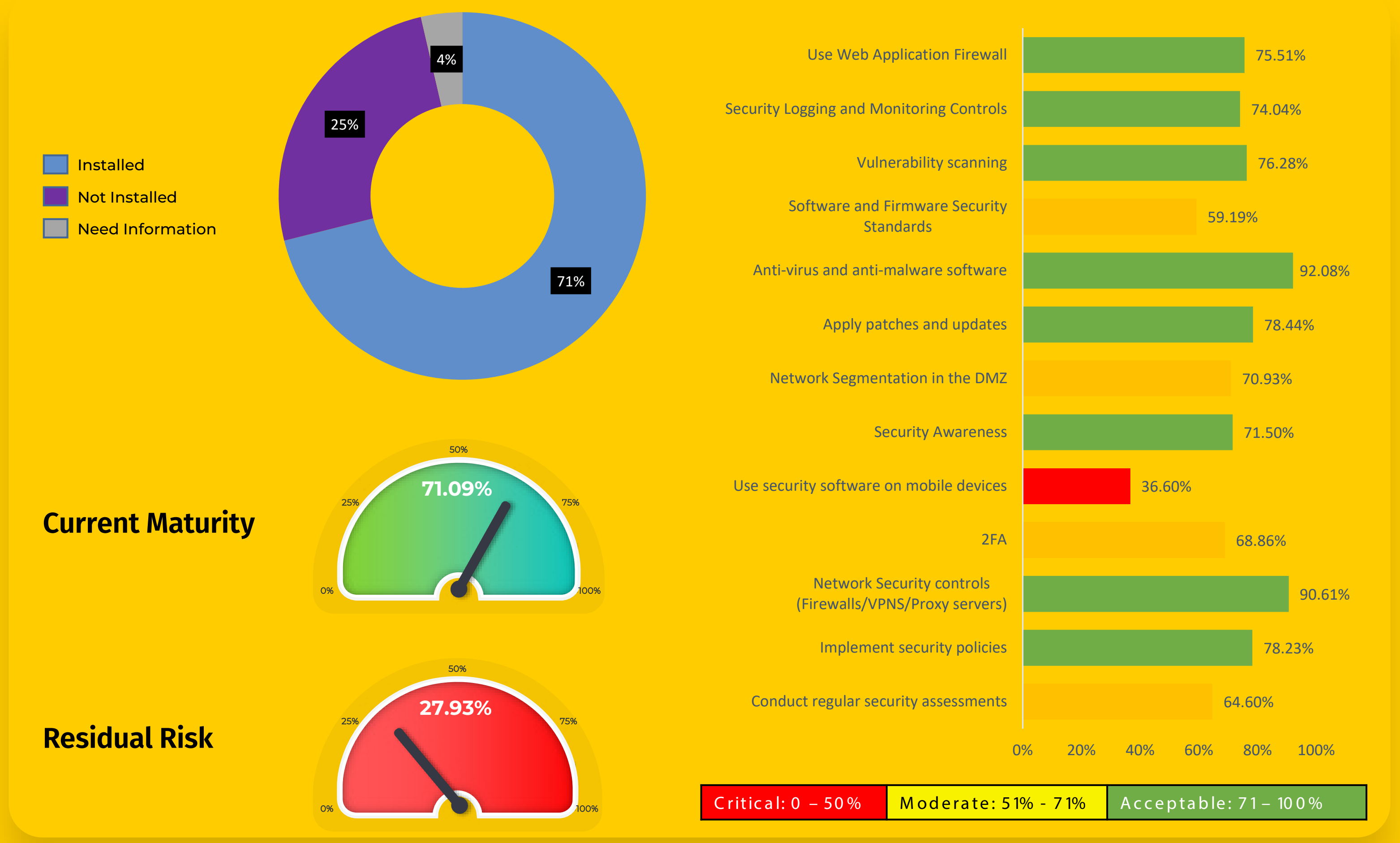

Figure 12 - T1133 - External Remote Services Detail

T1566 Phishing

Phishing is a method used by attackers to trick users into revealing sensitive information, such as usernames, passwords, credit card numbers, social security numbers, etc., typically by posing as a trustworthy entity. This could be through an email, website, or other communication methods that seem legitimate but are controlled by the attacker.

Attackers may send an email to a user pretending to be from a trusted source, such as a bank or a known contact, and lure the user into clicking on a malicious link or downloading a malicious attachment. Once the user interacts with these elements, the attacker can gain unauthorized access to the user's system or sensitive information.

Phishing is one of the most common and successful methods attackers use to breach security. It relies more on social engineering and exploiting human vulnerabilities than on exploiting software vulnerabilities. This technique does not require sophisticated technical skills and can be easily deployed at a scale, making it a favorite among attackers. There are various types of phishing, including Spear Phishing (T1566.001), where the attacker carefully crafts messages targeting specific individuals or organizations, and Clone Phishing (T1566.002), where a legitimate, previously delivered email is used as a template for creating an almost identical phishing message.

CONTROL	INSTALLED	NOT INSTALLED	NEED INFORMATION	T1189 - DBC
1. Security Logging and Monitoring Controls	807	249	34	74%
2. *Vulnerability Scanning*	804	228	22	76.3%
3. *Email Authentication Protocols*	784	181	41	77.9%
4. *Monitoring of social media and other platforms*	362	587	43	36.5%
5. *Software and Firmware Security Standards*	573	315	80	59.2%
6. *Browser Extensions*	748	145	32	80.9%
7. *Anti-virus and Anti-malware Software*	883	66	10	92.1%
8. *Security Awareness*	675	229	40	71.5%
9. *Use Security Software on Mobile Devices*	340	537	52	36.6%
10. *2FA*	648	260	33	68.9%
11. *Secure remote access*	748	145	32	80.9%
12. *Network Security Controls*	849	80	8	90.6%
13. *Anti-phishing software*	590	315	25	63.4%
14. *Spam filters/email content filtering*	795	124	13	85.3%
15. *Implement Security Policies*	726	161	41	78.2%
16. *Phishing incident response plan*	506	389	46	53.8%

T1566 Phishing

The survey results for T1566 (Phishing) provide some insight into the cybersecurity posture of the industry regarding this specific attack vector. The survey results highlight both the industry‘s strengths and areas for improvement in mitigating phishing attacks.

Significance of results

The analysis reveals that the industry has made significant strides in implementing critical controls such as Anti-virus and Anti-malware Software (92.1%) and Network Security Controls (90.6%), demonstrating a strong commitment to fundamental security measures. There are areas that require attention and improvement.

Organizations should prioritize the implementation of comprehensive anti-phishing measures to bolster their defenses:

» Employee Training: Conduct regular security awareness programs to educate employees on recognizing and reporting phishing attempts. This empowers individuals to become the first line of defense against phishing attacks.

» Email Authentication Protocols: Implement robust email authentication protocols to enhance protection against email-based attacks, reducing the risk of successful phishing attempts.

» Monitoring of Social Media and Other Platforms: Establish monitoring controls to detect and mitigate phishing threats originating from social media platforms, which are increasingly targeted by social engineering attacks.

» Phishing Incident Response Plan: Develop and regularly update a comprehensive incident response plan specifically tailored to address phishing incidents. This ensures prompt and effective handling of phishing attacks, minimizing their impact.

By prioritizing the recommended measures and combining technical controls, security awareness programs, and incident response procedures, organizations can enhance their readiness in combating phishing attacks.

Conclusions

70.4%

These results illustrate the industry‘s overall preparedness towards Phishing attacks and the specific controls currently in place to mitigate these attacks.

Organizations should prioritize the implementation of comprehensive anti-phishing measures, including employee training on recognizing and reporting phishing attempts. The use of advanced email authentication protocols and regular monitoring of social media and other platforms can help detect and mitigate phishing threats. Organizations should develop and regularly update a phishing incident response plan to ensure prompt and effective handling of phishing incidents.

T1566 - Phishing

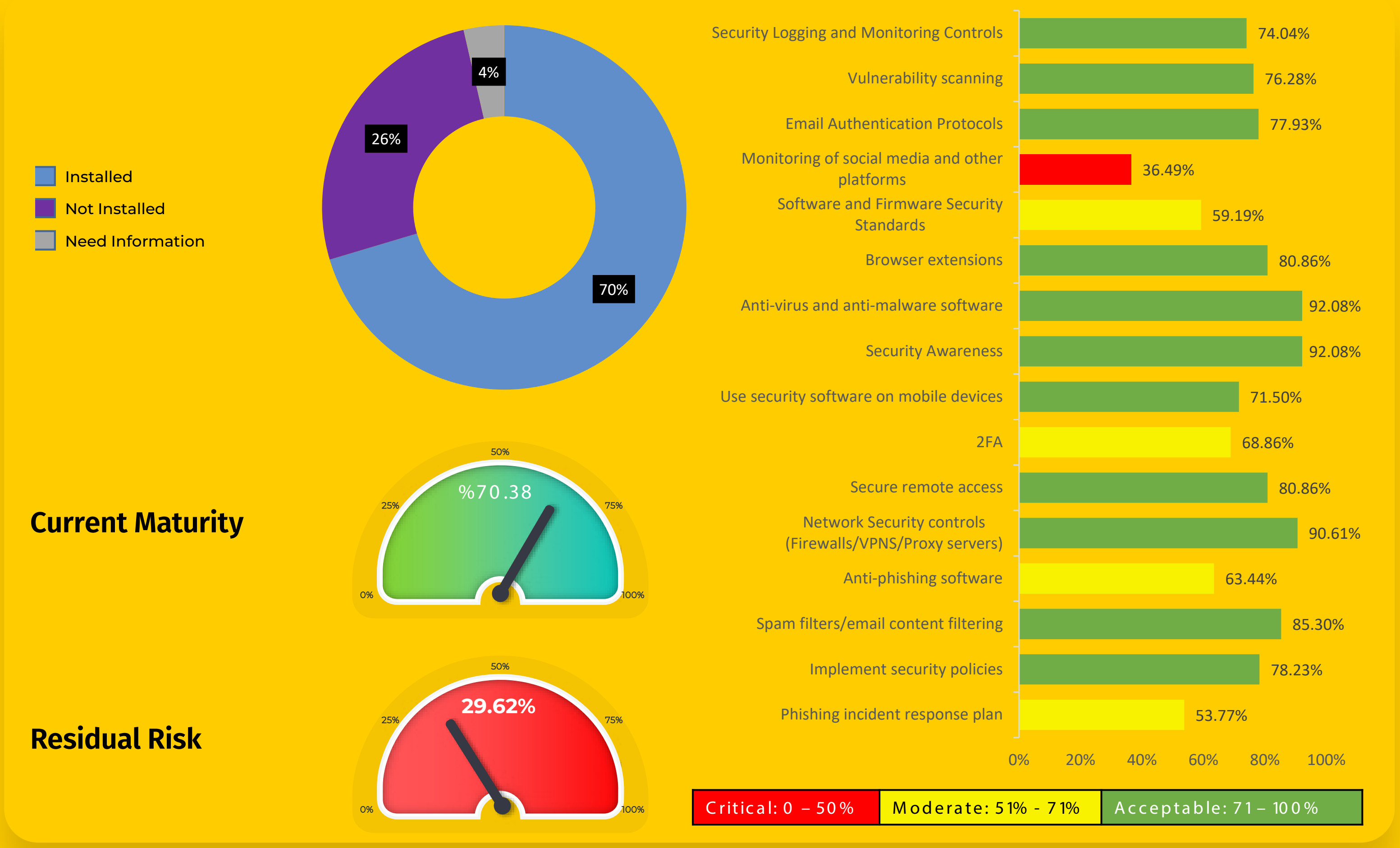

Figure 13 - T1566 - Phishing Detail

T1195 Supply Chain Compromise

Supply Chain Compromise involves the manipulation of products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. These manipulations can take many forms, including the use of third-party resources, components, software, or even system updates to inject malicious code or establish a foothold in a victim‘s environment.

This is an extremely severe form of cyberattack as it exploits the inherent trust between businesses and their suppliers. It can bypass traditional security measures by delivering the compromise from trusted sources, making it harder to detect and prevent.

Supply Chain Compromises are highly significant due to their potential for widespread damage, as seen in incidents like the SolarWinds hack, and recently, MOVEit!. They raise fundamental concerns about the security of third-party components in a networked world. The mitigation of this type of threat requires a holistic view of security that encompasses not just one‘s own systems, but also the systems of partners and suppliers.

CONTROL	INSTALLED	NOT INSTALLED	NEED INFORMATION	T1195 - SCC
1. Security Logging and Monitoring Controls	807	249	34	74%
2. *Apply Patches and Updates*	746	162	43	78.4%
3. *Network Segmentation in the DMZ*	671	245	30	70.9%
4. *2FA*	648	260	33	68.9%
5. *Network Security Controls*	849	80	8	90.6%
6. *Conduct Vendor Risk Assessments*	418	439	71	45%
7. *Secure communications/Secure Protocols*	694	190	44	74.8%
8. *Use encryption*	529	356	48	56.7%
9. *Implement Security Policies*	726	161	41	78.2%
10. *Conduct Regular Security Assessments*	604	296	35	64.6%

T1195 Supply Chain Compromise

It appears that there is strong adoption of several key controls to mitigate the risk of supply chain compromise, there are some areas, specifically vendor risk assessments and encryption usage, where the industry could increase its focus to improve its preparedness against this type of attack.

Significance of results

The survey results related to the T1195 - Supply Chain Compromise demonstrate an uneven level of preparedness across the industry.

Security Logging and Monitoring Controls, which play a vital role in quickly detecting and responding to a supply chain attack, is well-implemented, with 74% of respondents indicating their presence in their cybersecurity framework.

When we look at controls more specific to supply chain compromise, we see concerning trends with Conduct Vendor Risk Assessments, crucial in managing supply chain risks, yet only 45% of respondents have implemented it.

There is strong industry adoption of certain generic cybersecurity controls, but the data suggests a lack of readiness when it comes to measures that directly address supply chain compromise. This could potentially leave many organizations exposed to the risks associated with T1195.

There‘s a need for the industry to prioritize more specific controls, like Conducting Vendor Risk Assessments and implementing Encryption, to effectively combat supply chain attacks.

Conclusions

71.1%

It appears that there is strong adoption of several key controls to mitigate the risk of supply chain compromise, there are some areas, specifically vendor risk assessments and encryption usage, where the industry could increase its focus to improve its preparedness against this type of attack

Most organizations have prioritized Network Security Controls, such as firewalls, VPNs, and proxy servers. There is a notable need for improvement in conducting thorough vendor risk assessments. By assessing and managing risks related to vendors, organizations can enhance their supply chain security and reduce the potential impact of supply chain compromises.

T1195 - Supply Chain Compromise

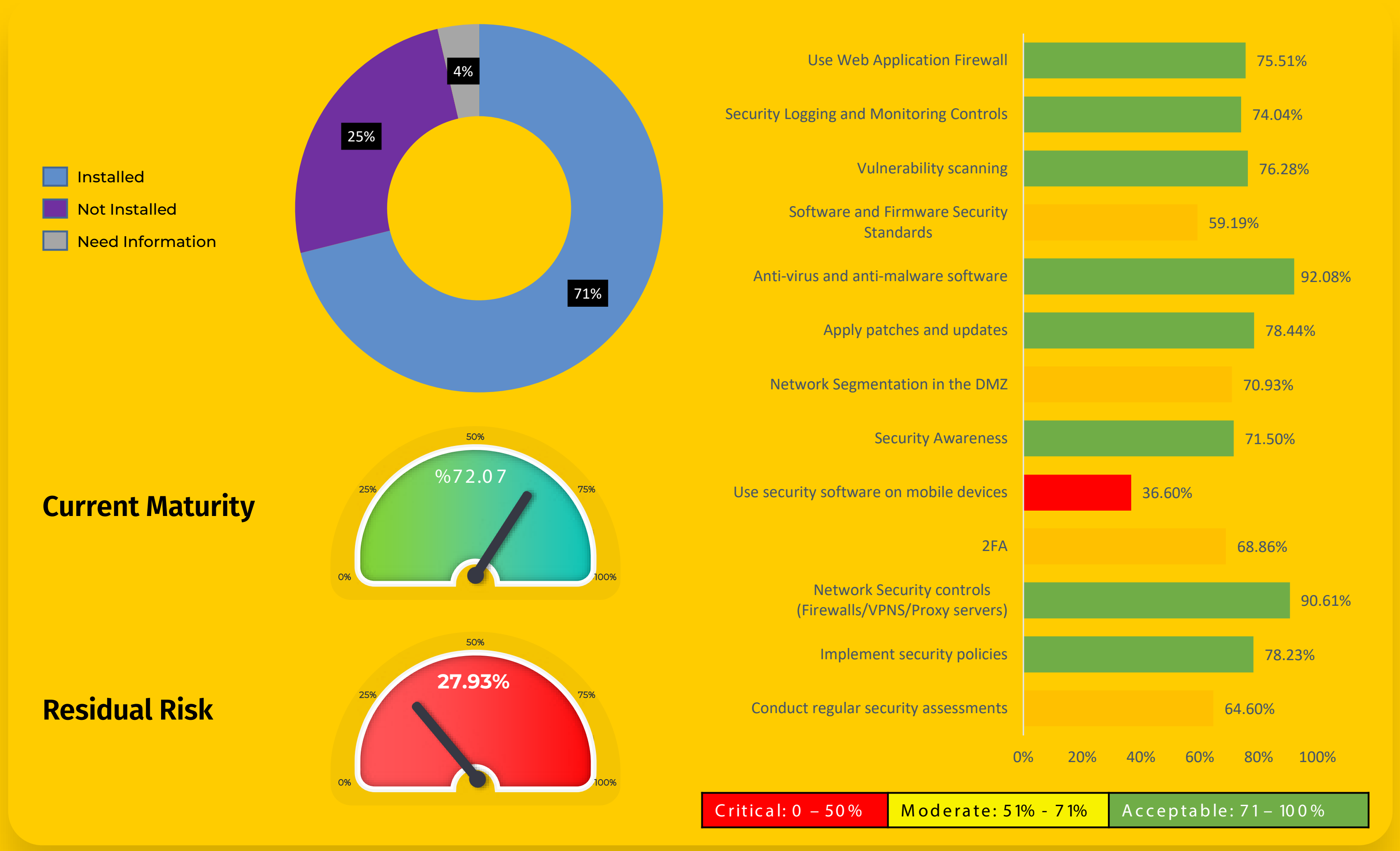

Figure 14- T1195 - Supply Chain Compromise Detail

T1199 Trusted Relationships

It involves the exploitation of trusted relationships between entities to gain unauthorized access or exploit vulnerabilities within an organization's network or systems. This tactic focuses on the manipulation or misuse of privileges, access rights, or connections that are considered trusted or legitimate.

Trusted relationships are crucial in business operations, as they enable collaboration, data sharing, and streamlined processes. However, attackers often target these relationships to bypass traditional security measures and gain unauthorized access. They may exploit the trust placed in external vendors, business partners, or even internal employees with elevated privileges to carry out malicious activities, such as data breaches, unauthorized system access, or spreading malware.

The importance of addressing T1199 lies in the fact that trusted relationships can serve as a significant attack vector, allowing adversaries to move laterally within a network, escalate privileges, and access sensitive information. By compromising trusted relationships, attackers can bypass traditional perimeter defenses and evade detection, making it essential for organizations to implement appropriate controls and strategies to mitigate the risks associated with these relationships.

CONTROL	INSTALLED	NOT INSTALLED	NEED INFORMATION	T1199 - TR
1. Security Logging and Monitoring Controls	807	249	34	74%
2. *Network Segmentation in the DMZ*	671	245	30	70.9%
3. *Security Awareness*	675	229	40	71.5%
4. *2FA*	648	260	33	68.9%
5. *Secure Remote Access*	748	145	32	80.9%
6. *Secure Communications/Secure Protocols*	694	190	44	74.8%
7. *Use Encryption*	529	356	48	56.7%
8. *Implement Security Policies*	726	161	41	78.2%
9. *Conduct Regular Security Assessments*	604	296	35	64.6%

T1199 Trusted Relationships

The results indicate a reasonable level of preparedness within the industry for managing trusted relationships. Most of the surveyed controls show a relatively high installation rate, suggesting that organizations are aware of the importance of implementing security measures in trusted relationships.

Significance of results

It is encouraging to see that a significant number of organizations have implemented foundational controls related to trusted relationships, such as security logging and monitoring, network segmentation, and secure remote access.

These controls demonstrate a proactive approach to threat detection, network isolation, and secure communication.

Organizations should prioritize the implementation of 2FA and similar authentication controls across their systems and applications. The use of encryption is another critical area that requires attention.

Regular security assessments are essential in evaluating the security posture of trusted relationships. By conducting thorough and frequent assessments, organizations can identify vulnerabilities, assess the effectiveness of implemented controls, and address any weaknesses promptly.

This proactive approach enables organizations to stay ahead of emerging threats and make informed decisions to enhance their security measures.

Conclusions

71.2%

Results indicate a moderate level of preparedness in terms of implementing controls related to trusted relationships (T1199). There is room for improvement in areas such as encryption and conducting regular security assessments. Enhancing these areas strengthen the industry's resilience against threats and mitigate the risks associated with unauthorized access or exploitation.

By focusing on the least implemented controls and working towards their adoption, organizations can enhance their preparedness for managing trusted relationships and reduce the associated security risks. Improving encryption practices can help safeguard sensitive data from unauthorized access and protect the integrity and confidentiality of information exchanged within trusted relationships.

T1199 - TRUSTED RELATIONSHIPS

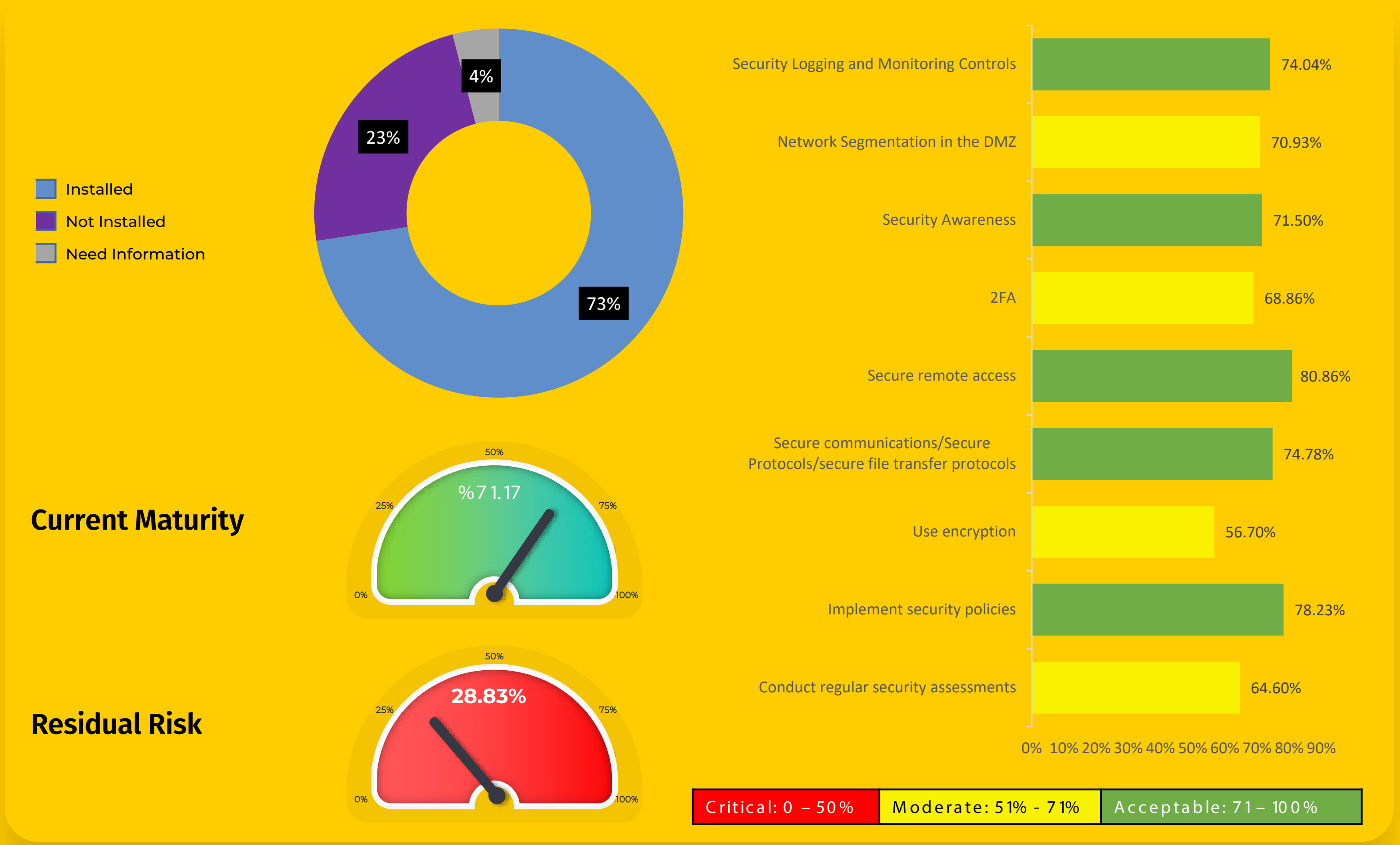

Figure 15- T1199 - Trusted Relationships Detail

T1078 Valid Accounts

T1078 is a tactic in the MITRE ATT&CK framework. It involves the abuse or compromise of valid user accounts to gain unauthorized access, move laterally within a network, or carry out malicious activities. Attackers often exploit weak passwords, stolen credentials, or misconfigured user accounts to gain a foothold within an organization's systems. Valid accounts are attractive targets for adversaries because they provide a legitimate entry point into an organization's network and systems.

By compromising valid accounts, attackers can bypass security controls and blend in with legitimate user activity, making their malicious actions more difficult to detect. This tactic can be used in various stages of an attack, from initial access to maintaining persistence within the target environment.

It is important to address T1078 (Valid Accounts) because the compromise of valid accounts can lead to significant consequences, including unauthorized access to sensitive data, disruption of critical services, and reputational damage. Organizations rely on user accounts for their daily operations, and a single compromised account can provide an attacker with a launching pad for further infiltration and lateral movement.

CONTROL	INSTALLED	NOT INSTALLED	NEED INFORMATION	T1078 - VA
1. Security Logging and Monitoring Controls	807	249	34	74%
2. *2FA*	648	260	33	68.9%
3. *Implement Security Policies*	726	161	41	78.2%

T1078 Valid Accounts

The results indicate that the industry is relatively well-prepared in addressing T1078 (Valid Accounts). The focus on security logging and monitoring controls and the implementation of security policies demonstrates a proactive approach to threat detection and mitigation.

Significance of results

By taking a proactive approach to user account security and prioritizing these additional security measures, organizations can effectively protect their systems and sensitive information from unauthorized access. The industry should continue to monitor emerging threats, adapt security controls accordingly, and foster a culture of continuous improvement to stay ahead of evolving cybersecurity risks.

Among the controls analyzed, the most implemented control is the implementation of security policies, emphasizing the importance of establishing guidelines and best practices for managing valid accounts.

The control with the lowest installation rate is two-factor authentication (2FA), potentially due to the implementation of more advanced authentication controls such as multi-factor authentication or additional controls within identity and access management programs.

Conclusions

73.7%

Results suggest that the industry has made progress in addressing T1078 (Valid Accounts) by implementing Security Logging and Monitoring Controls and Security Policies. Organizations should continue to prioritize the implementation of security measures to mitigate the risk of compromised accounts and minimize the potential impact of unauthorized access.

Organizations should consider implementing additional security measures such as privileged access management, following the principle of least privilege, and implementing multi-factor authentication. These measures help mitigate the risks associated with compromised or misused valid accounts.

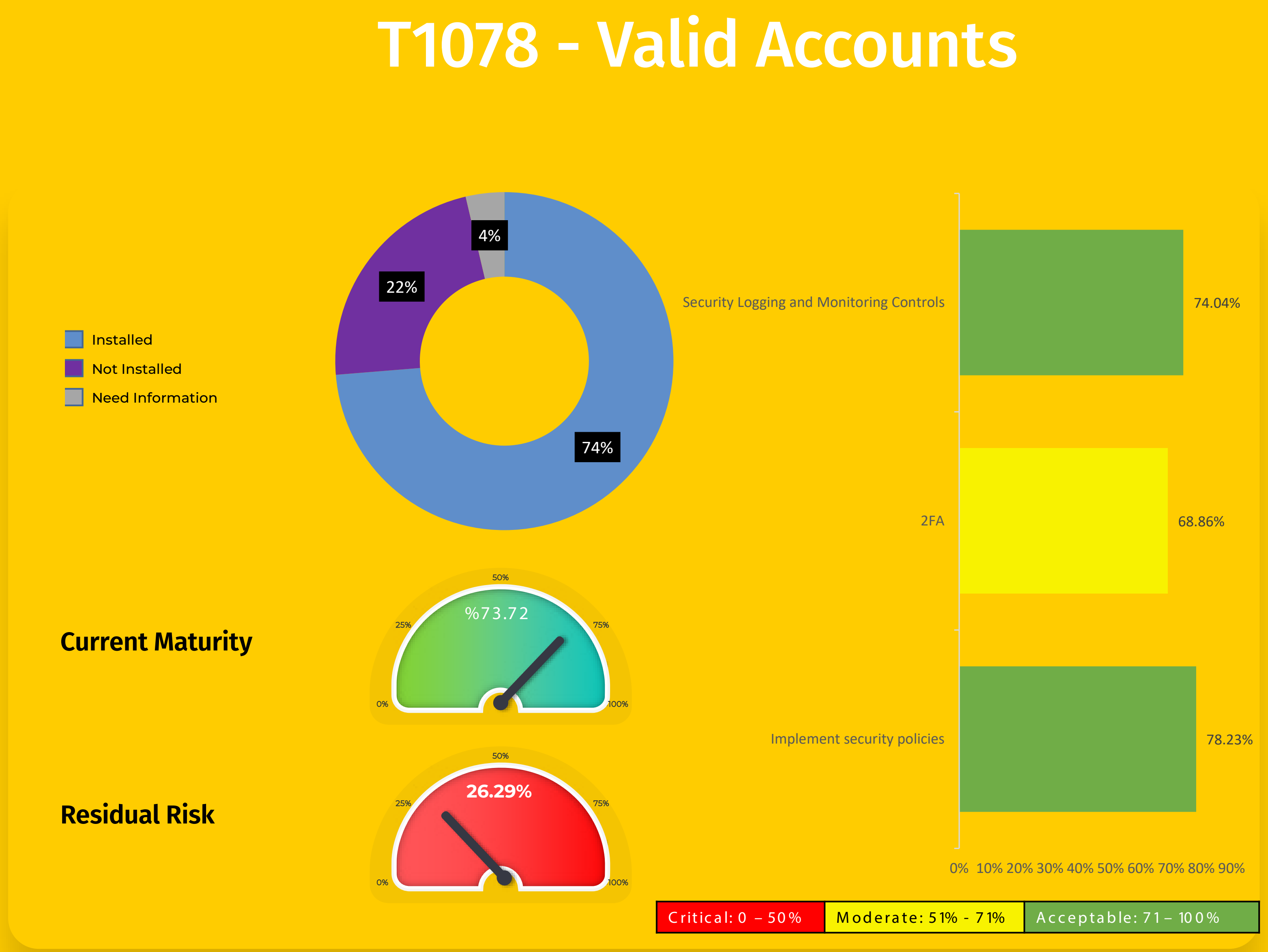

Figure 16- T1078 - Valid Accounts Detail

Conclusions and Recommendations

Our analysis has revealed some interesting insights into the cybersecurity controls organizations are implementing to detect and mitigate ransomware attacks.

For T1189 (Drive-by Compromise), T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1566 (Phishing), and T1078 (Valid Accounts), the most implemented control is Anti-virus and Anti-malware Software, with a consistent adoption rate of 92.1% across these threat categories. This shows that organizations recognize the importance of this basic but critical cybersecurity measure.

In the case of T1195 (Supply Chain Compromise), the most implemented control is Network Security Controls (Firewalls/VPNS/Proxy servers) with a 90.6% adoption rate, showing that most organizations understand the importance of network security in mitigating Supply Chain risks.

For T1199 (Trusted Relationship), the most implemented control is Secure Remote Access, showing an adoption rate of 80.9%. This reflects the fact that organizations are aware of the risks associated with remote access and are taking measures to secure it.

The least implemented control across T1189 (Drive-by Compromise), T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), and T1078 (Valid Accounts), is the use of Security Software on Mobile Devices, with a relatively low implementation rate of 36.6%. This indicates a significant gap in mobile device security among surveyed companies.

For T1566 (Phishing), the least implemented control is Monitoring of Social Media and other platforms with a 36.5% adoption rate. This shows that organizations need to pay more attention to social media platforms which can often be used for phishing attacks.

In the case of T1195 (Supply Chain Compromise), the least implemented control is Conducting Vendor Risk assessments, showing an implementation rate of only 45%. This suggests that many organizations may be neglecting an important aspect of supply chain security. For T1199 (Trusted Relationship), the least implemented control is the Use of Encryption, showing an implementation rate of 56.7%. This indicates a potential gap in protecting sensitive data often shared in trusted relationships.

Organizations seem to have adopted basic cybersecurity controls like Anti-virus and Anti-malware Software, but there are significant gaps in other areas such as Mobile device security, Social Media monitoring, Vendor Risk assessments, and the Use of Encryption. These areas should be focused on to improve the overall cybersecurity posture against ransomware attacks.

Interesting Observations

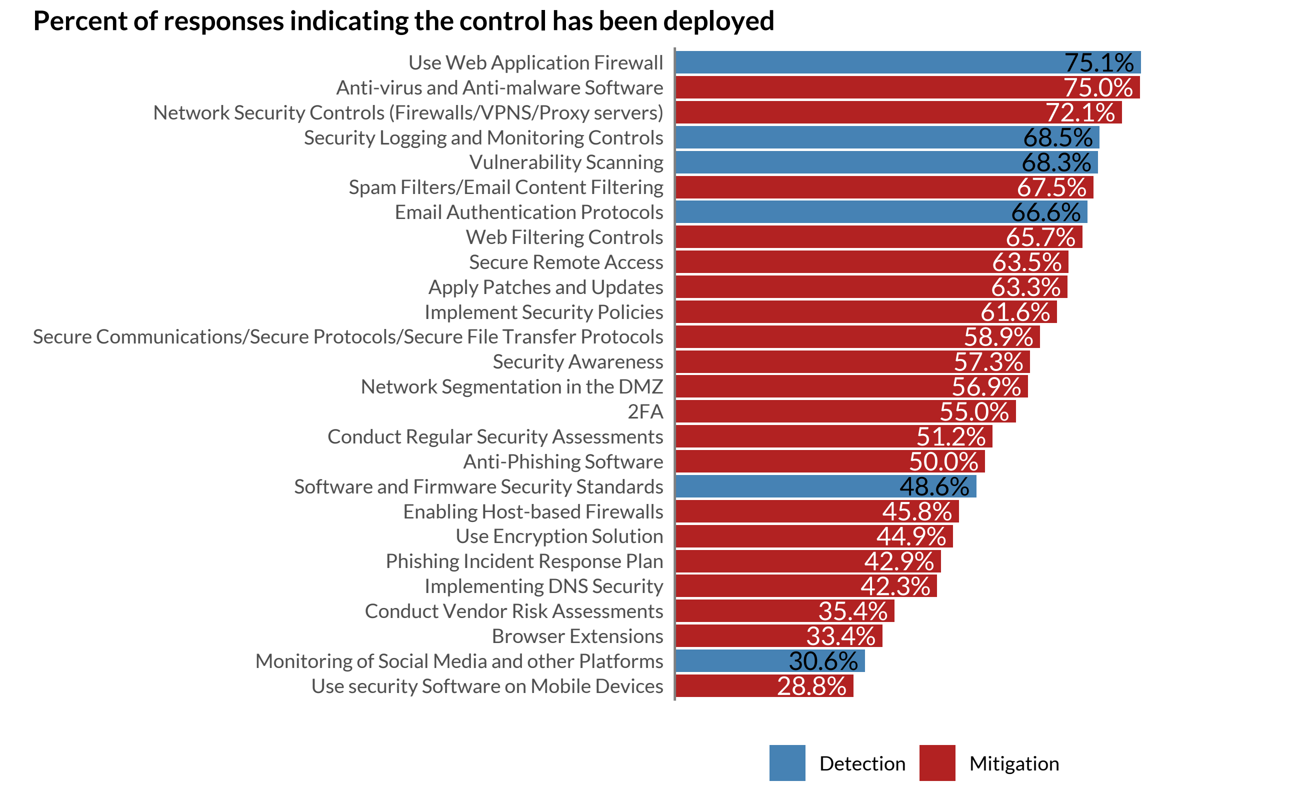

Figure 17 - Foundational controls deployed

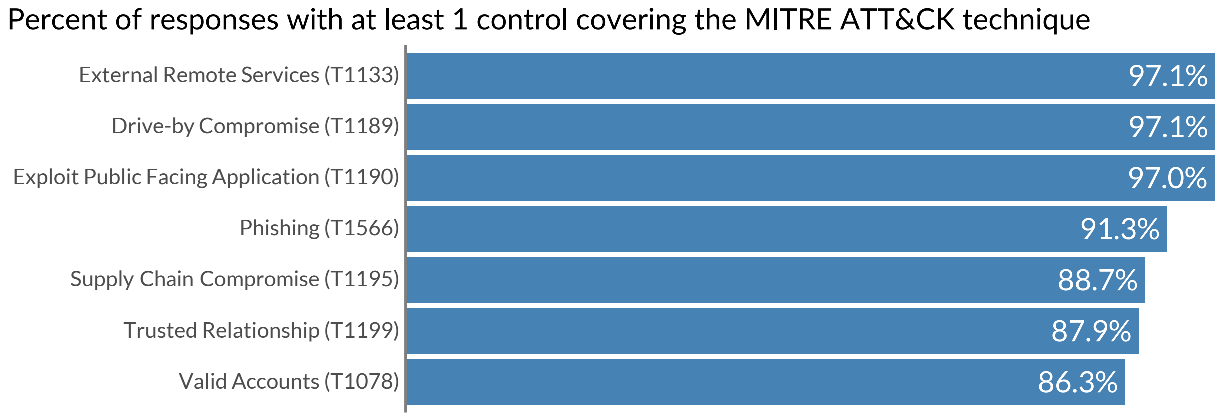

Figure 18 - One Foundational control for MITRE ATT&CK Technique

Interesting Observations

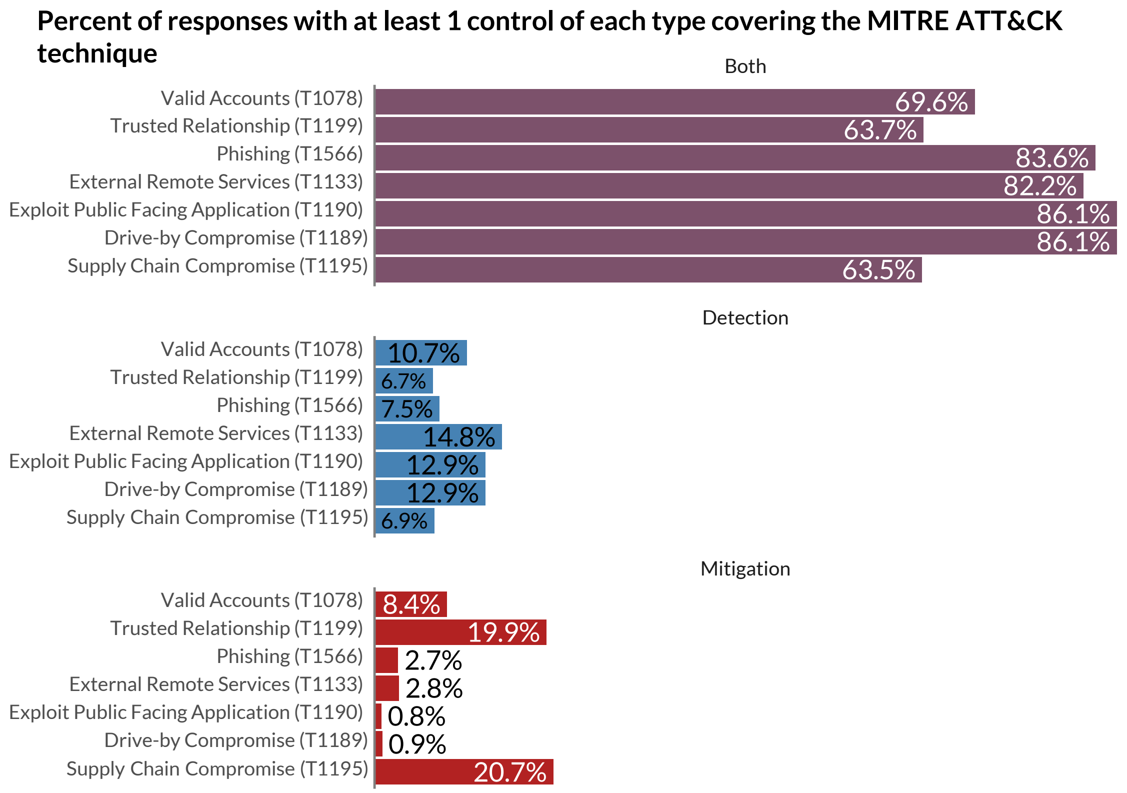

Figure 19 - Mitigation and Detection controls deployed

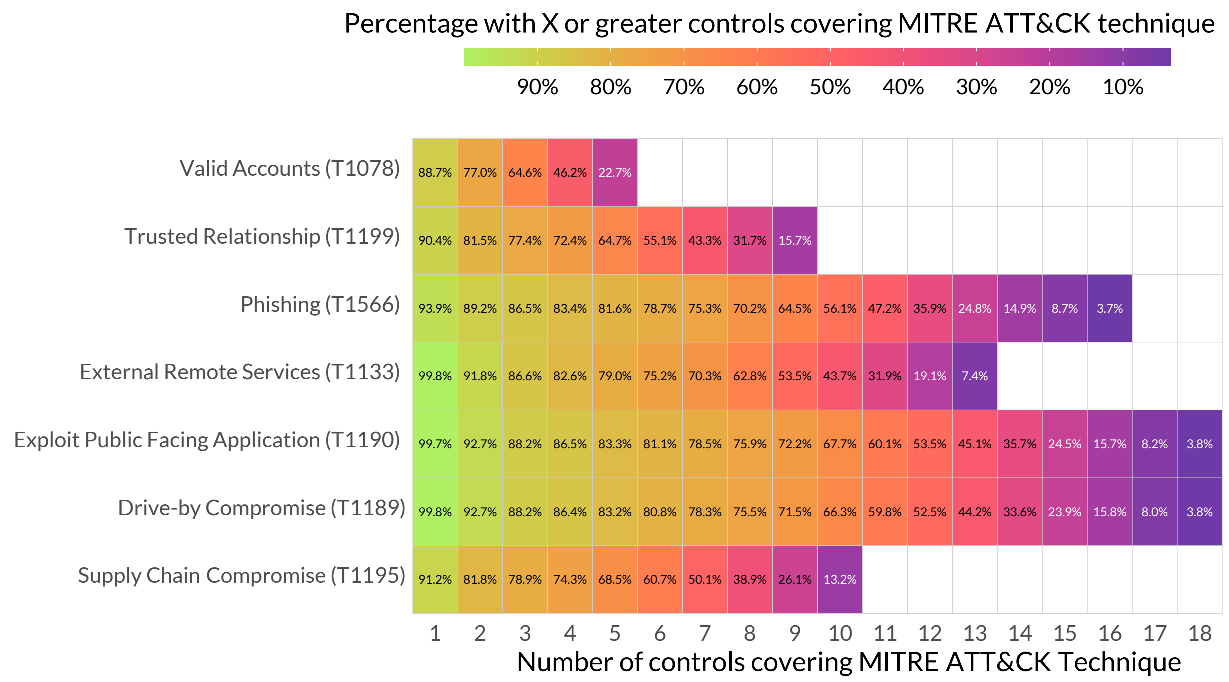

Figure 20 - Defense in Depth

Summary

In a constantly evolving threat landscape, maintaining a proactive and adaptable approach to cybersecurity is essential for organizations.

By prioritizing foundational controls and implementing comprehensive security measures, the industry can enhance its overall readiness, foster resilience, and safeguard against emerging cyber threats.

The goal of collecting and analyzing this information was to assess the industry's readiness and identify areas that require attention and improvement based on the Foundational controls identified in the Ransomware Control Matrix (RCX).

The industry's readiness regarding Foundational controls shows promise, but there is room for improvement. Organizations have demonstrated a good level of preparedness in implementing important controls such as Security Logging and Monitoring, Vulnerability Scanning, and Anti-virus and Anti-malware software. These controls are essential for proactive threat detection and protection against malware.

However, controls such as Vendor Risk Assessments, Two-factor Authentication, Encryption, and Regular Security Assessments exhibit lower implementation rates. Focusing on improving these gaps is important for enhancing the cybersecurity posture.

Continued vigilance, proactive monitoring, and a commitment to staying ahead of emerging threats are vital. By leveraging the insights gained from this analysis and implementing the recommended measures, organizations can enhance their defenses, better protect their critical assets and data, and mitigate the risks associated with ransomware attacks.

Thank you.

Thank you for taking the time to read this report. I hope that the information and insights provided have been of value to you.

I would like to extend my gratitude to the organizations and individuals who participated in the survey. Your contributions have been instrumental in generating this valuable data, and I am grateful for your collaboration.

I would like to thank my colleague, Aria Rahimi, for working with me in creating the Ransomware Control Matrix. Dr. Ben Edwards of Cyentia Institute for his time in reviewing the data and providing some really interesting insights (see charts pages 36 & 37). Ryan English and Andres Almanza for their support in reviewing and encouragement to publish these findings.

And to all the CISOS in Latin America that are part of the CISOS LATAM SUMMIT community, thank you for your time and your valuable input and recommendations.

I encourage organizations to leverage the findings and recommendations presented in this report. I hope that the information presented here will contribute to a safer and more secure digital landscape for all.

Ed Rojas
www.rcxmatrix.org

References

4. Ransomware Control Matrix
   a. https://rcxmatrix.org
5. MITRE ATT&CK
   a. https://attack.mitre.org/
6. MITRE D3FEND
   a. https://d3fend.mitre.org/
7. T1189 – (Drive-by Compromise)
   a. https://attack.mitre.org/techniques/T1189/
8. T1190 (Exploit Public-Facing Application)
   a. https://attack.mitre.org/techniques/T1190/
9. T1133 (External Remote Services)
   a. https://attack.mitre.org/techniques/T1133/
10. T1566 (Phishing)
    a. https://attack.mitre.org/techniques/T1566/
11. T1195 (Supply Chain Compromise)
    a. https://attack.mitre.org/techniques/T1195/
12. T1199 (Trusted Relationship)
    a. https://attack.mitre.org/techniques/T1199/
13. T1078 (Valid Accounts)
    a. https://attack.mitre.org/techniques/T1078/
14. WAF
    a. https://www.indusface.com/blog/top-threats-a-web-application-firewall-can-mitigate/
    b. https://www.radware.com/products/appwall/
15. Security Login and monitoring
    a. https://www.crowdstrike.com/blog/detecting-and-responding-to-ransomware-how-logging-everything-helps-mitigate-ransomware-risks/
    b. https://www.cisa.gov/stopransomware/ransomware-guide
16. Vulnerability Scanning
    a. https://owasp.org/www-community/Vulnerability_Scanning_Tools
    b. https://www.beyondtrust.com/resources/glossary/vulnerability-scanning
17. Email Authentication Protocols
    a. https://www.upguard.com/blog/email-security
    b. https://www.emailonacid.com/blog/article/email-deliverability/email-authentication-protocols/
18. Monitoring of Social Media and other Platforms
    a. https://www.cisa.gov/sites/default/files/publications/NCSAM_SocialMediaCybersecurity_2020.pdf
    b. https://media.defense.gov/2021/Aug/06/2002824387/-1/-1/0/CSI_KEEPING_SAFE_ON_SOCIAL_MEDIA_20210806.PDF
19. Software and Firmware Security Standards
    a. https://csrc.nist.gov/csrc/media/Publications/white-paper/2022/02/24/getting-started-with-cybersecurity-risk-management-ransomware/final/documents/quick-start-guide--ransomware.pdf
    b. https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf

References

20. Web Filtering
    a. https://www.paloaltonetworks.com/blog/network-security/ransomware-attacks-advanced-url-filtering/
    b. https://www.cisa.gov/stopransomware/ransomware-guide
    c. https://expertinsights.com/insights/how-to-stop-ransomware-attacks/
21. Browser Extensions
    a. https://www.microsoft.com/en-us/edge/learning-center/everything-to-know-about-browser-extensions
    b. https://brave.com/learn/what-are-web-browser-extensions/
22. Anti-Virus and Anti-Malware Software
    a. https://www.malwarebytes.com/
    b. https://www.avast.com/c-ransomware-protection-tool
23. Apply Patches and Updates
    a. https://www.rapid7.com/fundamentals/patch-management/
    b. https://www.cyberdot.com/cyber-security/the-importance-of-patches-and-updates/
24. Network Segmentation in the DMZ
    a. https://www.techtarget.com/searchsecurity/definition/DMZ
    b. https://guillermo-roman.com/network-security-part-5-network-segmentation-dmz/
25. Security Awareness
    a. https://securityawareness.usalearning.gov/
26. Use Security Software on Mobile Devices
    a. https://www.verizon.com/articles/device-protection/mobile-device-security/
    b. https://www.ibm.com/topics/mobile-security
27. Enabling Host-based Firewalls
    a. https://climbtheladder.com/10-host-based-firewall-best-practices/
    b. https://security.berkeley.edu/MSSND/host-based-firewall-software-guidelines
28. Implementing DNS Security
    a. https://authenticweb.com/guides/a-complete-guide-to-managing-dnssec/
    b. https://www.cloudflare.com/learning/dns/dns-security/
29. 2FA
    a. https://www.okta.com/blog/2021/07/what-is-two-factor-authentication-2fa/
    b. https://www.techtarget.com/searchsecurity/definition/two-factor-authentication
30. Secure Remote Access
    a. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf
    b. https://www.parallels.com/blogs/ras/remote-access-security-best-practices/
31. Network Security Controls (Firewalls/VPNS/Proxy servers)
    a. https://www.cisco.com/c/en/us/products/security/what-is-network-security.html
    b. https://www.ztna-hub.com/what-is-network-security-controls/
32. Anti-Phishing Software
    a. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing
    b. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection-about?view=o365-worldwide

References

33. Spam Filters/Email Content Filtering
    a. https://techgenix.com/complete-guide-email-spam-filters/
    b. https://learn.microsoft.com/en-us/exchange/antispam-and-antimalware/antispam-protection/content-filtering?view=exchserver-2019
34. Conduct vendor risk assessments
    a. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/vendor-risk-management
    b. https://www.sans.org/security-awareness-training/resources/vendor-risk-management
35. Secure Communications/Secure Protocols/Secure File Transfer Protocols
    a. https://www.baeldung.com/cs/transfer-files-protocols
36. Use Encryption
    a. https://www.techwell.com/techwell-insights/2019/10/importance-data-encryption-cybersecurity
    b. https://www.infoguardsecurity.com/importance-of-encryption-in-cybersecurity/
37. Implement Security Policies
    a. https://www.varonis.com/blog/what-is-a-security-policy
    b. https://www.ibm.com/docs/en/i/7.3?topic=policies-implementing-policy
38. Conduct Regular Security Assessments
    a. https://www.ena.com/articles/6-reasons-you-should-conduct-regular-security-assessments/
    b. https://blog.plazaprotection.com/safeguard-your-business-reputation-conduct-regular-security-assessments/
39. Phishing Incident Response Plan
    a. https://www.sans.org/security-awareness-training/resources/phishing-incident-response-plan

Ransomware Control Matrix (RCX)

2023

Industry Analysis of Foundational Controls

www.rcxmatrix.org