ISACA®

PROACTIVE CYBERSECURITY

A Quick Guide to Understanding Cyber Maturity

Foreword by ISACA®

FOREWORD

by ISACA

According to a report from Skybox Security, "Vulnerability and Threat Trends Mid-Year Report 2021," the amount of ransomware attacks grew by nearly 20% and new vulnerabilities in operational technology (OT) devices increased by 46%. In the time of COVID-19, cybercrime is not only surviving, but also thriving.

As digital transformation continues to accelerate at a rapid pace and the availability of the talent required for such advancement decreases, cyberattacks are not likely to go away any time soon.

So, what can organizations do to protect themselves in an ever-evolving technological landscape that's prone to further and further attacks? How ready are your cybersecurity defenses? The time to mature your operational cybersecurity is here.

Cybersecurity maturity is the term that refers to the ability and readiness of an organization to protect itself against possible vulnerabilities and cyber threats. In general, the more mature your organization's cybersecurity protective practices are, the better equipped it is to prevent threats.

Maturity models provide the framework to measure the company in question's level of maturity. Ratings are given for each domain based on its preparedness to cyberattacks. These ratings often showcase which areas are sufficient and which are in need of improvement. A "0" rating indicates the organization doing the absolute bare minimum to protect itself while a "5" rating would suggest the company is employing the best practices and controls to detect and prevent cyber threats.

These assessments are crucial should an organization want to gain significant insights into their own security practices and their relative effectiveness. The results often can improve communication between IT personnel and upper management and can be used to enhance existing and implement new cybersecurity protocols in lacking areas.

As far as when a company should take a cybersecurity maturity assessment, there is no wrong time. However, many organizations are struggling to administer a maturity assessment or implement new and/or recommended protocols and practices due to the lack of available talent in the industry.

Gartner reported in a recent study that IT executives see the talent shortage as the most significant adoption barrier to 64% of emerging technologies, compared with just 4% in 2020.

Even based on these results, it remains unclear for the time being how much worse cyberattacks could potentially become in the coming years or how much these skill gaps could widen. But if IT leaders want to correct organizational vulnerabilities amid the talent shortage, it may be time to start becoming a bit more proactive in their approach.

To help you become more proactive and understand cyber maturity to its fullest, we put together this compendium containing the expertise and know-how of leading cybersecurity professionals. Discover how to build cyber resilience with risk-based solutions to measure, assess and report on cyber maturity based on current industry standards.

And enjoy!

Cyber Maturity and
Protecting Against Ransomware

SUBMITTED BY TOM CONKLE
CISSP, Optic Cyber Solutions

Ransomware continues to dominate the headlines in both cybersecurity journals and mainstream media. Companies of all sizes across sectors are seeing continued increases in ransomware attacks. This rise in attacks has resulted in companies paying out millions of dollars or, in some cases, failing due to the irreparable harm caused by the loss of ransomed data. Ransomware attacks will continue to increase primarily due to the successful monetization of attacks and because ransomware methods continue to evolve.

Ransomware began with attackers simply gaining access to, and encrypting, a company's data. This enabled the attackers to sell a decryption key back to the company to allow them to regain access to company data. Ransomware has since evolved. One method includes taking over a company's access control features and locking users out of systems until the victim pays the ransom. Attackers have even been known to weaponize regulators. After breaching company data and requesting payment, attackers will threaten to notify the regulators themselves if not paid.

Attacks that lead to ransom payments being demanded have been realized through multiple attack methods. One of the first ransomware attacks reported in 1989 occurred when an AIDS researcher distributed 20,000 floppy disks infected with malware to attendees at a World Health Organization (WHO) conference. The malware has been used to exploit known and zero-day vulnerabilities to allow access to systems as a vector for ransomware. Malware used in ransomware attacks has been deployed through many methods, including social engineering attacks (e.g., phishing), seeding parking lots with infected USB drives, and even exploiting publicly available systems. Other forms of ransomware have occurred due to companies unknowingly leaving their data exposed to the internet, allowing attackers to steal or encrypt the data.

Due to the variety of forms of ransomware and the many ways it can be deployed, a single solution does not exist. Companies must take a holistic view of their cybersecurity program and implement capabilities across the entire program.

Organizations need to defend their infrastructure on all fronts to thwart ransomware attacks. First, the organization must ensure the development and integration of secure solutions within their environment. For example, when purchasing new Software as a Service (SaaS) capabilities, companies should safeguard systems by changing defaults passwords, hardening configurations, deploying cloud protection capabilities (e.g., Cloud Access Security Broker (CASB)), and implementing Multi-Factor Authentication (MFA). While each of these protections may not prevent a successful ransomware attack alone, a multipronged approach to defending against ransomware reduces the chance of an attacker's success.

Organizations also need to implement robust protective technologies to ensure systems are routinely patched and vulnerabilities are managed. Additionally, to provide a defense-in-depth approach, the organization must enable effective auditing and logging to allow early detection of potential breaches that could lead to a ransomware attack. While an attacker only has to be successful once to implant their ransomware malware, organizations must effectively defend their network at all times, across all aspects of their cybersecurity program.

There are many resources available to assist organizations in defining a robust cybersecurity program. For starters, there are various industry accepted cybersecurity guidelines, such as the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (the Cybersecurity Framework), and the Center for Internet Security (CIS) Common Security Controls (CSC). Additionally, there are many regulatory and compliance requirements across sectors, such as the Payment Card Industry (PCI) Data Security Standard (DSS), the Health Insurance Portability and Accountability Act (HIPAA), and North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP). There are also tools, such as ISACA's CMMI Cybermaturity Platform (CCP), that measure current cybersecurity capabilities and recommends specific solutions needed to mitigate organizational business risks.

The CCP tool includes 16 Capability Areas that represent a full cybersecurity program. Each area assists organizations in defining cybersecurity capabilities needed to manage operational risk, including the risk of a ransomware attack. The CCP Cybersecurity Model ("the Model") identifies key proficiencies to help organizations prevent ransomware within its Capability Areas, including System Trustworthiness and Protective Technology. The Model also defines specific actions, referred to as Practices, that companies can take to detect ransomware before it spreads in the Incident Detection and Continuous Monitoring Capability Areas.

The holistic approach for implementing a maturity-based cybersecurity program, as realized in the CCP, enables companies to evaluate risks to establish tailored Target Maturity Levels. The CCP then translates these Target Maturity Levels into Practices that can be implemented to mitigate their cybersecurity risks to an acceptable level, including the risk of ransomware disrupting business operations. Additionally, the Model within the CCP is updated bi-annually to ensure cybersecurity capabilities evolve with ever-changing threats and vulnerabilities.

Editor's note:
Find out more information about CCP here.

10 Tips for Talking **Cybersecurity With Your Board**

ISACA's CMMI® Cybermaturity Platform makes cyber resilience—and more effective conversations with your board—possible. Aligned with leading security frameworks like NIST, its assessment generates a unique risk profile for your organization, prioritizes gaps in capabilities, identifies the maturity required to achieve your organizational goals, and recommends options to address the gaps. With this data in hand, ISACA's CMMI Cybermaturity Platform builds your board's confidence and trust by aligning strategic objectives with pragmatic insights into cybersecurity risks.

To learn more about the CMMI Cybermaturity Platform or schedule a demo, visit www.isaca.org/cmmi-cybermaturity-platform.

A recent study from global technology association ISACA found that 87% of C-suite professionals and board members lack confidence in cybersecurity initiatives. How can you talk to your board in a way that builds trust and gains buy-in caused by the loss of ransomed data. Ransomware attacks will continue to increase primarily due to the successful monetization of attacks and because ransomware methods continue to evolve.

1

Know your organization's cybersecurity risks.
Ensure that you've identified and documented all of the potential risks facing your organization. With strong communication and documentation, it will be easier to obtain support for risk mitigation efforts.

2

Communicate your organizational risks effectively.
Understanding your risks is good—but being able to effectively communicate them to stakeholders is better. Don't just tell leadership what the concerns are—provide context and illustrate potential effects in terms of financial impact or damage to your brand reputation. Ensure that you've identified and documented all of the potential risks facing your organization. With strong communication and documentation, it will be easier to obtain support for risk mitigation efforts.

3

Know your security controls.
Understand what security controls are in place within the organization, ensure they are documented and understand their efficacy. Don't forget, security controls can take many forms, from technical tools to organizational processes such as incident response plans, or people such as physical security guards.

4

Communicate security control needs.
Make sure that stakeholders are aware when a certain control needs more attention or funding. Gaining buy-in from leadership will ensure critical controls are maintained. Effective communication describing the security control needs to the board will help illustrate the importance of investing in these valuable preventative measures.

5

Show fiscal relevance.
Boards need to understand what kind of financial commitments are required to support a mature cybersecurity posture. Illustrating how cutting-edge cyber trends can impact the bottom line may be the make-or-break factor for board approval.

6

Communicate business impact.
Effectively articulate best- and worst-case scenarios to leadership. Providing this type of awareness will ensure that boards understand what is at stake, should an incident occur.

7

Have a plan.
Illustrate how changes made within an organization can increase organizational cyber maturity. Provide a roadmap, with concrete action plans and dates, to show how a stronger cyber stance is achievable. Document the risk mitigation efforts, explaining the reasoning for pursuing specific risks over others—remember, it is okay to only address certain risks, if they are directly applicable to your organization and are documented as such.

8

Illustrate improvement in cyber maturity.
Present growth over time to the board. Demonstrate how implementing previous controls made the organization more resilient. Make the illustration personal by focusing your lens on the specific needs of the organization. Contextualized improvement consistently outweighs abstract growth.

9

Encourage tenacity.
Over time, as an organization's cyber maturity increases, fewer catastrophic incidents may occur. Encourage the board to continue its dedication to staying cyber strong and maintaining funding and personnel. One effective method of encouragement is through continuous evaluation, demonstrating that the need for a strong cyber posture is constant.

10

Stay data-driven and transparent.
Even if the truth hurts, it is important that boards have an honest understanding of the organization's cyber maturity levels (or lack thereof). Only through transparency can they address cyber threats head-on.

Genuine Parts Builds **Improved Cyber Maturity** with ISACA's CMMI® Cybermaturity Platform

SUBMITTED BY ISACA NOW

Genuine Parts Company determined that its initial cyber maturity assessment needed to create a baseline against a common framework that aligns with NIST CSF and the ISO 27001 controls. Genuine Parts needed to assess multiple units, demonstrate maturity that was aligned with the NIST CSF, and specifically focus on demonstrating maturity performance in managing risk; not just compliance-based.

Genuine Parts Company determined that its initial cyber maturity assessment needed to create a baseline against a common framework that aligns with NIST CSF and the ISO 27001 controls.

Genuine Parts needed to assess multiple units, demonstrate maturity that was aligned with the NIST CSF, and specifically focus on demonstrating maturity performance in managing risk; not just compliance-based.
Genuine Parts customized the CMMI Cybermaturity Platform to target these specific areas for improvement in their assessment.

- Apply governance elements
- Apply risk strategy
- Implement risk management
- Implement risk identification
- Ensure access control management
- Apply data security protection
- Apply organizational training
- Ensure trustworthy systems
- Apply operational protection provisions
- Apply protection planning
- Apply protective technology provisions
- Apply cybersecurity incident detection
- Apply continuous monitoring
- Apply incident response
- Apply incident handling
- Apply incident recovery

The Solution
Genuine Parts selected the CMMI Cybermaturity Platform because of its alignment with globally recognized standards, particularly the NIST Cyber Security Framework (CSF), as it is already an industry benchmark with risk-based controls, as well as its Informative References and alignments across the 20 CIS (Center for Internet Security®) Cyber Security Controls, COBIT Controls, ISA–62443-2-1–2009 (Security for Industrial Automation and Control Systems), ISO/IEC 27001 INFOSEC Controls, and the federal controls NIST SP 800-53 Rev. 4 -1 provide additional utility. To succeed, Genuine Parts determined that its initial CMMI Cybermaturity Platform maturity assessment model be:

- Digital
- Risk-based
- Provide a risk profile/map
- Easy to use
- Customizable
- Self-paced
- Align to the NIST Cyber Security Framework (CSF)
- Align to the ISO 27001 Controls for ease of self-assessment and improvement
- Produce a roadmap for improvement

"THIS VIEW PROVIDED SPECIFIC INSIGHT FOR MEASURED VS. TARGETED MATURITY LEVELS - AN EYE-OPENING EXPERIENCE AND **A RALLYING CRY FOR ACHIEVING CONTINUOUS IMPROVEMENT**"

As Genuine Parts developed its customized risk profile, the descriptors for each frequency of occurrence values led to invaluable discussions among the Genuine Parts senior leaders. Without these definitions, calibrating their current state and then defining improvement goals would have been nearly impossible.

In addition, using the CMMI Cybermaturity Platform Maturity Scorecard within each Practice Area Assessment allowed employees to review and understand the People, Process, and Technology (PPT) objective for each maturity level, and its relative ISO 27001 Informative Reference by Maturity Level. This view provided specific insights for measured vs. targeted maturity levels—an eye-opening experience and a rallying cry for achieving continuous improvement.

Key Performance Goals Achieved
While the Genuine Parts Company Enterprise Security Team could not control the number of security incident tasks it received, it could control how it handled their resolution in a more efficient and timely manner.

Since the CMMI Cybermaturity Platform self-assessment in January 2020, they have:

- Reduced Mean Time to Task Resolution (MTTR) from nearly 24 days (23.9) over the previous three quarters to an average of 6.5 days for the first two quarters in 2020
- Decreased the range of Backlog Days for Tasks from as high as 117 days during the previous three quarters, to a low of six days for the first two quarters in 2020

Editor's note: Read the full Genuine Parts case study. For additional resources on cyber maturity, including a video on how ISACA's CMMI® Cybermaturity Platform helps CISOs, CIOs, and large enterprise organizations build cyber maturity, visit ISACA's cyber maturity page.