WHITE PAPER

Future-Proof Your Security Maturity

SecureTrust™
a Trustwave® division

Overview

As cybersecurity threats continue to grow more sophisticated, organizations must move beyond simply putting security programs in place and begin to look around corners, adapting and improving these programs to address the threats of tomorrow.

But just as teenagers must take algebra before advancing to calculus, organizations must improve their key security processes and capabilities so they can continually implement more sophisticated and efficient measures. Just as students must mature in their academic capabilities before tackling advanced coursework, security teams must usher their programs through a development process before instituting thoughtfully layered defense-in-depth cybersecurity approaches.

The problem is that many companies don't have a complete picture of their current security posture, nor do they understand what's required to move ahead. That's because the typical measures of a security program—the number of tickets closed each month, volume of vulnerability scans without critical findings or annual compliance assessments to meet regulatory or industry standards—offer merely binary reporting: You meet the bar, or you don't. Counting vulnerabilities closed or the number of attacks successfully mitigated is part of the picture, but the numbers alone do not provide a holistic measure of your vulnerability management program's performance—nor do they indicate the maturity level of your security organization.

This is where security maturity modeling comes in. By helping organizations assess their current operational effectiveness and determine how to improve their performance, these models offer a roadmap and empower companies to assess and achieve their security objectives. A security maturity model provides the framework for measuring your security program, offers context to determine the appropriate maturity level for your goals and serves as a scaffold to support your efforts to progress to a more sophisticated security posture.

When you assess your Payment Card Industry Data Security Standard (PCI DSS) compliance with SecureTrust, we include security maturity scoring for critical security categories and by PCI DSS Prioritized Approach security milestones. This allows you to benchmark and improve your security operations, as well as communicate with senior leadership and obtain sponsorship to make incremental improvements according to your goals.

In this white paper, we'll delve deeper into security maturity, examining:

- The history of security maturity frameworks and why they matter.
- The value of integrating security maturity frameworks into investment and compliance programs to achieve business goals.
- The benefits of security maturity to your business and how it can span different compliance frameworks.

The Evolution of Security Maturity Models

What we know today as security maturity models trace their history back to the 1980s.

As organizations adopted computerized systems through the 1960s and '70s, the demand for software development exploded. As a result, developers raced to meet demand without clear parameters or best practices, and failures became common. Many projects ran over budget and over schedule, while a few programming errors—including those involved in Therac-25 radiation therapy machines produced in the early 1980s—actually killed people. When several U.S. military programming projects failed to meet their objectives, the U.S. Department of Defense funded research to create the Capability Maturity Model (CMM), intended to formalize and improve business processes around software development. This model was updated in 2006 with the Capability Maturity Model Integration (CMMI) roadmap.

Since 2012, new maturity models have been developed and updated specifically to address cybersecurity best practices—first for critical infrastructure and later for all sectors. These include the Cybersecurity Capabilities Maturity Model (C2M2), the National Institute of Science and Technology (NIST) Cybersecurity Framework (CSF) and the Department of Defense Cybersecurity Maturity Model Certification (CMMC).

Today, organizations from many different industries rely on these maturity models to measure their business processes and cybersecurity capabilities.

How We Define Security Maturity

At SecureTrust, we measure the maturity of seven security categories, aligning with common security best practices and compliance frameworks. They are:

Boundary Defense

- Firewalls, personal firewalls, proxies, demilitarized zone (DMZ) perimeter networks and network-based intrusion detection and prevention systems (IDS/IPS)
- Secure configurations for boundary defense tools

Asset Management

- Inventory of authorized and unauthorized devices
- Secure configurations for network devices, hardware and software assets

Application Software Development and Security

- Antivirus and malware defenses
- Data lifecycle management

User Management

- Controlled use of administrative privileges
- Account monitoring and control

Data Protection

- Encryption and data loss prevention (DLP)
- Controlled access based on the need to know

Security Testing and Monitoring

- Maintenance, monitoring and analysis of audit logs
- Vulnerability management, penetration tests, red teaming and incident response

Training

- End-user training
- Security staff skills development

In addition to the security category, SecureTrust measures your maturity with respect to the PCI DSS security milestones from the PCI Security Standards Council Prioritized Approach to help stakeholders understand where they can reduce risk earlier in the compliance process. The PCI DSS security milestones are:

- **Milestone 1:** Remove sensitive authentication data and limit data retention
- **Milestone 2:** Protect systems and networks, and be prepared to respond to a system breach
- **Milestone 3:** Secure payment card applications
- **Milestone 4:** Monitor and control access to your systems
- **Milestone 5:** Protect stored cardholder data
- **Milestone 6:** Finalize remaining compliance efforts, and ensure all controls are in place

Our security maturity model consists of a systematic program of increasingly organized and more advanced levels to enable organizations to improve performance and key capabilities. For each security category and each PCI DSS security milestone, you will be scored from zero to five as follows:

0. **INCOMPLETE:** An incomplete process is ad hoc or unknown.
1. **INITIAL:** An initial process is unpredictable and poorly controlled.
2. **REPEATABLE:** A repeatable process is planned and controlled but is often still reactive.
3. **DEFINED:** Proactive rather than reactive, defined processes are documented and standardized.
4. **MANAGED:** Managed processes are quantitatively managed to improve in pursuit of performance objectives.
5. **OPTIMIZED:** Optimized processes are continuously improved to respond to opportunity and change

The Danger of Immaturity

As cyberthreats grow perpetually more sophisticated, your cybersecurity efforts must follow suit. However, new SecureTrust data shows that organizations are actually *decreasing* in maturity across all seven security categories. In 2020, the average maturity score for each category declined to less than a 3, meaning the average organization's cybersecurity processes are not documented and standardized. The Data Protection category leads with a maturity score of 2.54, down from 2.80 last year. Security Testing and Monitoring, meanwhile, performed worst, declining to an average of 2.45 from 2.61.

What's behind this dismal performance? A major problem is the lack of periodic reviews. Regular reviews are critical to ensure that executives are working through the compliance implications of business changes and adjusting their security approach accordingly. Without regular attention, key cybersecurity processes will not be successfully managed and will fail to satisfy their intended objectives over the long-term.

Even as average security maturity scores fall, the PCI DSS and other payment card industry security frameworks continue to push ahead, evolving to keep up with changes in technology, threats and vulnerabilities. This creates an ever-growing divide between a typical organization—one honestly pursuing compliance, but without complete insight into the maturity of their processes relative to peers and without objectives of their own—and the expectations of regulatory bodies.

Many companies attempt to achieve PCI DSS compliance by deadline but fail to maintain compliance throughout the year and across all control areas. Most compliance lapses result because organizations are not using defined, authorized processes or taking small steps toward process improvement and continuous compliance. Some merchants and service providers become entangled in a never-ending game of whack-a-mole in which they rush to fix an issue ahead of the annual assessment but then fail to maintain compliance throughout the year until threatened again with the possibility of a non-compliant assessment. Moreover, some companies continue to rely on manual processes or process with single points of failure that could undermine the entity's overall PCI DSS compliance status—a potentially very expensive problem.

What's the Ideal Level of Maturity?

The ideal maturity will depend on an organization's specific priorities and risk appetite. The end goal is to determine and implement this organization-appropriate level rather than to blindly seek the highest possible level for every company. To determine your objectives and set a course for achieving your desired maturity level, it's important to select the maturity model or framework best suited to your business. This involves considering the purpose and audience of the model as well as the model's limitations—or flexibility—when applied within your business.

That said, we recognize the benefits of moving forward with any model over getting stuck trying to determine the best specific model, because adopting a model is just the first step. Comparing one to another is of secondary importance to the main act of launching a security maturity improvement initiative. Indeed, most of the cybersecurity models mentioned earlier, though developed for specific industries, are broad enough to be utilized by any organization. For example, the C2M2 was created by the U.S. Department of Energy for use by utility companies, but it can be tapped by any company to benchmark the maturity of their cybersecurity operations.

Rather than focusing on the best model, it may be more useful to compare your maturity level to that of similar organizations. SecureTrust has a large and growing database of security maturity scores across a range of industries. With this data, we can provide actionable insights by measuring maturity levels relative to the seven security categories, the PCI DSS security milestones and how you stack up against your peers. As a result, you can see where you might be over or underinvested depending on the maturity of your compliance processes and your goals.

Conclusion

Increasingly sophisticated threat actors will continue to target data, creating ever-evolving tricks and techniques to stay ahead of cybersecurity efforts. Companies of all sizes must first understand their security operations' strengths and weaknesses to begin the process of improving them.

Security maturity modeling offers a framework by which to monitor, measure and communicate your organization's security capabilities—and then to move to the next level, beginning the continuous improvement process that allows you to constantly improve your security posture, become more resilient to threats and effectively fight back against the bad actors who threaten your organization's future.

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com