ORIGINAL FINDINGS

2019 Global Compliance Intelligence Report

SecureTrust™
a Trustwave® division

PCI DSS Compliance Intelligence Report

Overview

A security maturity model provides the framework for measuring the maturity of a security program and guidance on how to reach the next level—a foundation for a path forward in an organization's security management. A security maturity model can be a valuable tool for improving your cyber security efforts. It enables your organization to periodically assess where it is along that path to maturity and is a useful benchmark to communicate with upper management for support. A maturity model helps organizations assess the current operational effectiveness of key processes and helps entities figure out what capabilities are needed to improve their performance.

The Payment Card Industry Data Security Standard (PCI DSS) provides a baseline of technical and operational requirements designed to protect account data. The standard itself acknowledges that the "PCI DSS comprises a *minimum* set of requirements for protecting account data and may be enhanced by additional controls and practices to further mitigate risks." Organizations must determine for themselves which, if any, additional controls and practices should be in place to further mitigate risk.

SecureTrust provides Compliance Intelligence; maturity scoring to help clients gain an understanding of their process maturity relative to peers and their own objectives. SecureTrust Compliance Intelligence is derived from maturity ratings built into our PCI DSS Compliance Validation Service. Compliance Intelligence data has been anonymized and published in this report for use by merchants and service providers to gain an understanding of maturity across industries and regions.

In this white paper, we consider:

- Compliance Intelligence defined
- Compliance Intelligence data sources
- Security maturity data by industry and control area
- Compliance Intelligence in your organization

Executive Summary

- The fundamental benefit of a maturity model is that it establishes a framework for continuous process improvement.
- The ideal maturity level for an organizational control will depend on the specific priorities and risk appetite of the entity in question.
- For security and privacy, organizations should of course seek to satisfy minimum requirements and then understand what the incremental improvements in maturity are to achieve effective data management.
- Maintaining compliance is the major challenge that could be mitigated with repeatable processes managed toward known performance objectives.
- SecureTrust assessors are still seeing manual PCI DSS controls in place and merchants and service providers are failing requirements they have met in the past.
- There is room for improvement in each control area. No single control area advanced to a maturity ranking of four (4) or managed.
- E-commerce has the highest overall rating as an industry and has the top maturity score. But the top score was only 3.01, barely reaching the defined maturity level. Each other industry category scored lower, squarely in the repeatable maturity level with scores from 2.14 - 2.84.
- Ease of implementation is not the determining factor in the maturity ratings for a control area.
- Maturity ratings by control area show an overall failure in the management of processes to meet their intent. A major issue is lack of periodic reviews to ensure the successful management of key processes and to verify that the process continues to satisfy the intended objective.

Compliance Intelligence Defined

What is Compliance Intelligence?

In short, Compliance Intelligence refers to maturity scoring to help clients gain an understanding of the maturity of their processes relative to peers and their maturity objectives.

To say more, Compliance Intelligence is when individuals in your organization have complete information. Compliance Intelligence is when decision makers gain an understanding of compliance status, their controls and the maturity of their practices. Compliance Intelligence is when an organization has been empowered and knows how to talk about evaluating their compliance investment and tradeoffs according to their organization's unique maturity objectives.

Compliance Intelligence Maturity Levels

SecureTrust maturity levels are designed to enable organizations to improve performance, key capabilities and critical business processes. Our maturity model consists of an evolutionary path of increasingly organized and systematically more mature processes. The fundamental benefit of a maturity model is that it establishes a framework for continuous process improvement:

0) INCOMPLETE: Ad hoc or unknown process.

1) INITIAL: Initial approach to carrying out a 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: Processes are quantitatively managed to improve toward performance objectives.

5) OPTIMIZED: Processes are continuously improved to respond to opportunity and change.

Compliance Intelligence Control Areas

SecureTrust measures the maturity of eight key organizational control areas, chosen for their applicability to common compliance frameworks.

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

Facility Controls:

- Security testing and monitoring
- Maintenance, monitoring, and analysis of audit logs

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

What's Mature Enough?

The ideal maturity level for an organizational control area will depend on the specific priorities and risk appetite of the entity in question. We believe you should consider implementing processes at a maturity level sufficient to mitigate the risks to achieving your organizations objectives within a control area.

As a start, we suggest that no organization should risk failing their PCI compliance assessment. Further, we recognize that maintaining compliance is the major challenge that could be mitigated with repeatable processes managed toward known performance objectives. Accordingly, for the SecureTrust Compliance Intelligence model, an organization should strive for a baseline maturity level of at least 3.5 on the scale of 5 outlined previously.

Why the Need for Security Maturity?

Immature practices. SecureTrust assessors are still seeing manual PCI DSS controls in place.

Compliance lapse. Merchants and service providers are failing requirements they have met in the past. Staff transition is a common reason for a lapse in compliance when new employees do not understand the PCI requirements and their role. Or worse, management of the requirements completely falls off.

Moving with the times. The PCI DSS and related payment card industry security frameworks are maturing. Technology, threats and vulnerabilities are continually evolving. Businesses should re-assess compliance and process maturity periodically and in response to any significant changes.

New business demands. Organizations must consider the compliance implications of mergers, acquisitions and other major business changes. Businesses must understand where the acquired entity stands in their compliance program or understand the impact on compliance of significant changes to operations. Planning ahead is an act of maturity.

New regulations. In addition to security frameworks, regulatory frameworks for privacy are in effect or being developed, including the General Data Protection Regulation (GDPR) governing processing of personal data and the California Consumer Privacy Act (CCPA) governing the sale of consumer data. For security or privacy, there are minimum requirements and then there are incremental improvements in maturity that should be considered to achieve effective data management.

Compliance Intelligence Data Sources

Our Data

As the most commonly selected Qualified Security Assessor in the world for PCI and payment related assessments, SecureTrust has a large and growing database of security maturity ratings across industries and regions from which to derive Compliance Intelligence.

This report examined the maturity of over 400 organizations from PCI DSS assessments taking place over a twelve month reporting period from July 2018 to June 2019.

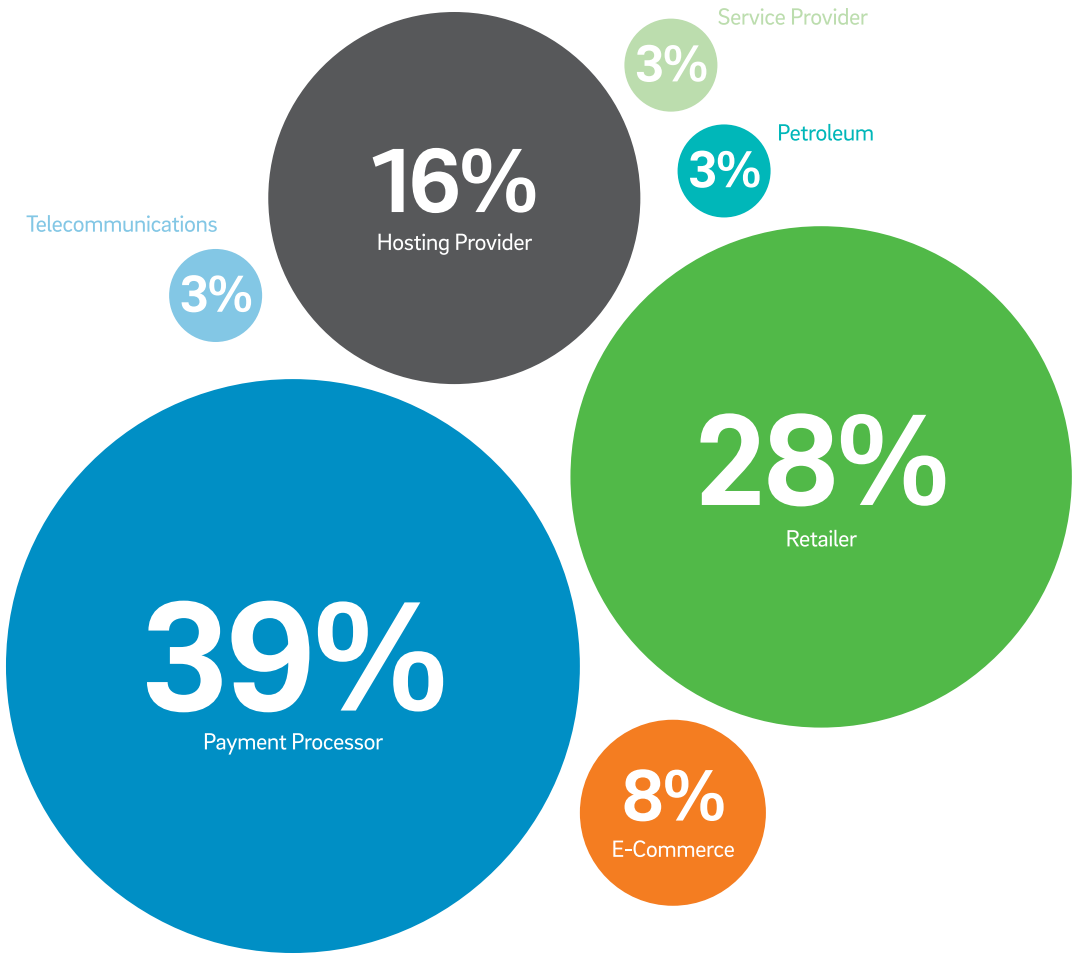
Industry Demographics

The 2019 Compliance Intelligence data comes from seven industry categories, listed here in order of maturity:

- E-commerce
- Telecommunications
- Service Provider
- Retailer
- Payment Processor
- Petroleum
- Hosting provider

The industry most frequently represented in our data is the payment processor category followed by the retail industry, which stands to reason given their large volumes of payment transactions requiring a third party validation of PCI compliance. The next largest category is hosting providers, followed by ecommerce, petroleum, telco's and other service providers.

By Industry

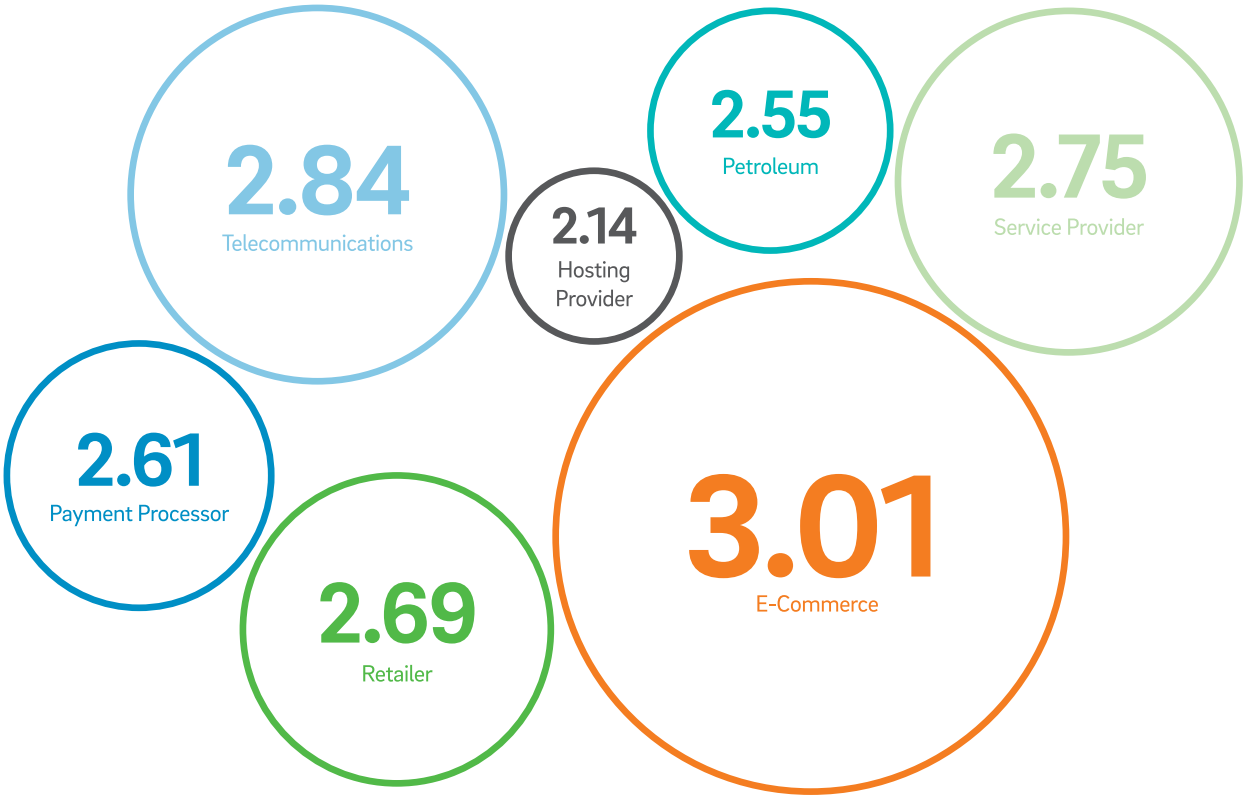

Service Provider
3%
Petroleum
3%
16%
Hosting Provider
Telecommunications
3%
28%
Retailer
39%
Payment Processor
8%
E-Commerce

Maturity by Industry and Control Area

Maturity by Industry

E-commerce has the highest overall rating as an industry and has the top maturity score for each of the eight control areas. With a maturity score of 3.01, E-commerce barely reached the Defined maturity level, where processes are proactive, defined, documented and standardized. The next step up in maturity will be to develop performance objectives and improve toward them.

All other industry categories score between 2.14 and 2.84, squarely in the Repeatable maturity level range. The Hosting Provider category ranks the lowest, with a score of 2.14. This score is indicative of the increase in the number of small, hosting provider organizations entering the market who have not matured their processes.



E-commerce

Uniting security and privacy for e-commerce and mobile transactions will only help to enable the continued use and growth of wireless software, content and commerce. Alternatively, a failure to provide security and privacy will diminish consumer adoption rates with one vendor over another.

Due to the rise in e-commerce transactions and an increased focus on the security of online transactions, it makes sense e-commerce scored best in our research findings. However, we would expect Data Protection, Boundary Defense and User Management maturity scores to be higher, as they should be viewed as critical control areas.

Telecommunications

Theft of user credentials is up.[1] User management and the controlled use of administrative privileges should be a primary focus area for telecommunications and other organizations handling sensitive data. And, especially important in consideration of credentialed access and permissions for data stored and managed in multitenant cloud environments.

As we discuss later, our research found inconsistent password and authentication controls, weak administrative access controls, and use of generic accounts and shared credentials.

Service Provider

Service Providers are playing an important role in the overall security of the entities they serve. Given the vital role, we anticipate the level of scrutiny and demands of security to increase over time. The more partners and customers they have, the more mature they will have to become in their processes. Some organizations have misaligned incentives and there is evidence that some organizations seek merely to gain a report on compliance, as opposed to conducting an honest, thorough approach to assessing compliance obligations and security implications of their actions.

Boundary Defense and Asset Management are two control areas we would expect to perform higher, both of which should be improved as critical elements of their third-party services role.

Retail

Asset Management is the control area that rated the lowest maturity for the retail industry. Management of point-of-sale systems is a ramp up challenge with newer and smaller merchants. Change management processes are also in need of oversight and consistency. Evaluations for asset management and change control are reflected in the overall retail industry rating.

[1] *https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/*

Payment Processor

The payment processor industry includes organizations such as the payment card brands, banks and payment gateways that are under a lot of scrutiny for their data security. It might be expected that the overall maturity scores for these organizations would lead the industry list. Note, however, that the ratings are lower than would be expected, specifically for Boundary Defense and Security Testing and Monitoring. Boundary Defense includes secure network configurations and firewall protection and Security Testing and Monitoring includes continuous vulnerability assessment, penetration tests, incident response and remediation.

Petroleum

The computers and networks that control energy delivery are different than desktop configurations. The systems are designed for dependable and continual flow of power, and these differences should be taken into consideration when securing networks. Improvements have been made in hardening of systems and reducing the number of available ports and services. But application software security and training need improvement as vulnerabilities can be found in old and new systems alike.

Hosting Provider

More and more organizations are trusting hosting providers[2] with their most sensitive data. And, like every new trend or technology, there are upsides and downsides. Of course, accessibility and mobility are advantages enabling business to perform tasks from anywhere at any time. Alternatively, organizations must be vigilant to protect against risks to the confidentiality and integrity of the data

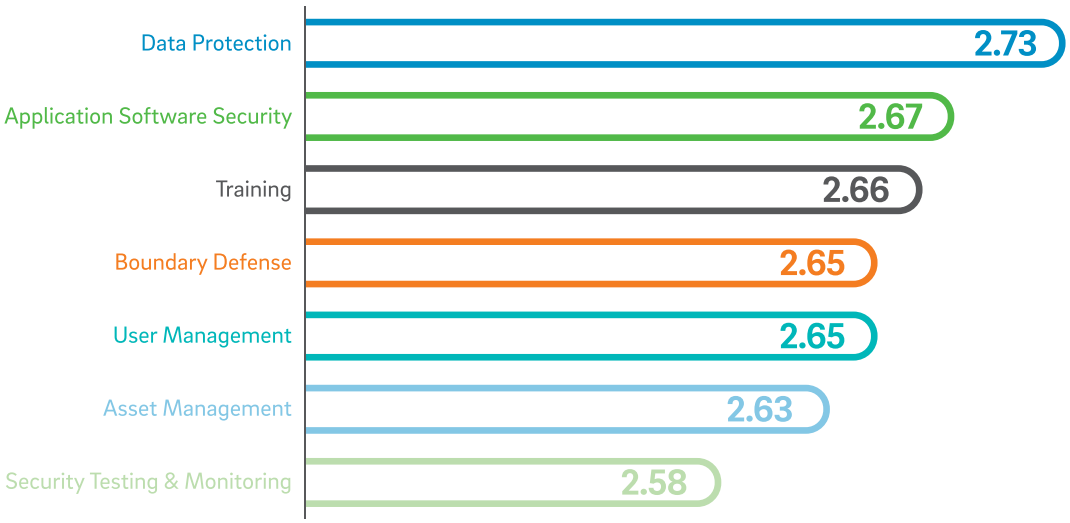
[2] *https://www.flexera.com/blog/cloud/2018/02/cloud-computing-trends-2018-state-of-the-cloud-survey/*

Maturity by Control Area

There is room for improvement in each control area. Many processes are still manually performed. No single control area advanced to a maturity ranking of three or Repeatable. Rather, each control area scored in the 'Initial' maturity category range, characterized as an unpredictable and poorly controlled approach to carrying out a process. The next step in maturity will be for organizations to develop a planned and controlled approach to make the processes at least 'Repeatable'.

Ease of implementation is not the determining factor in the maturity ratings for a control area. For instance, Data Protection and Application Software Security score higher than Training in maturity. Relative to other control areas, Training should be a simpler control area to achieve because the bar is lower than that of some of the more difficult controls. For instance, it's easier to periodically conduct security awareness training than it is to develop a robust security testing and monitoring program to follow the best practices laid out in the training. It's easier to provide training on application software security than it is to perform secure coding. We posit that Training maturity should be higher because it's, both, an easier control to achieve and it pays dividends for other control areas when employees have been trained and know the importance of their role in the overall compliance program.

Maturity ratings by control area show an overall failure in the management of processes to meet their intent. A major issue is lack of periodic reviews to ensure the successful management of key processes and to verify that the process continues to satisfy the intended objective.



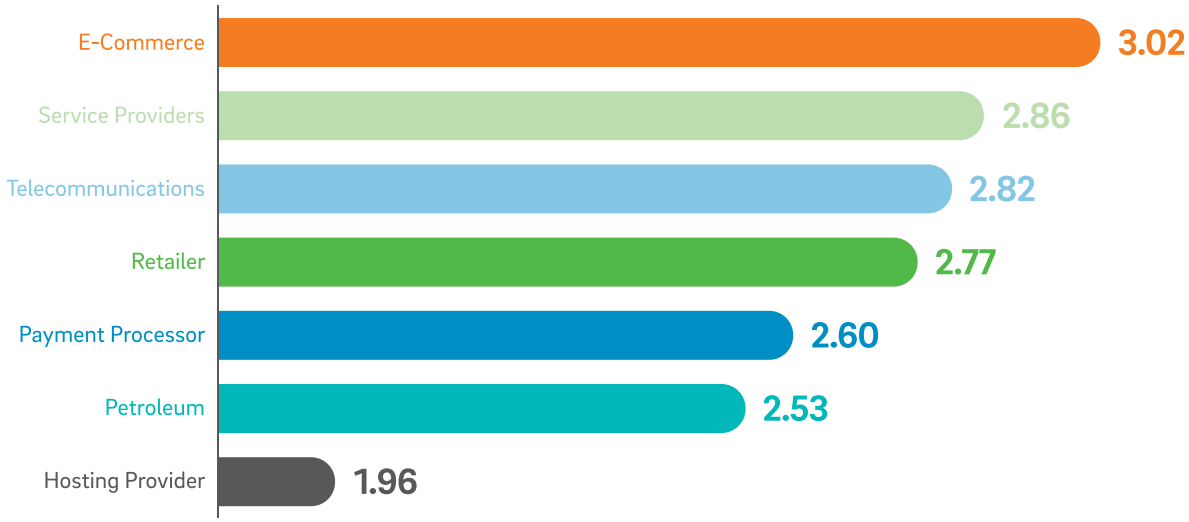
Boundary defense

Hackers attack the boundary because, from across the internet, they can reach the DMZ and workstations that are pulling data through network boundaries. Configuration and architectural weaknesses at the perimeter, on network devices, internet facing machines and partner networks are used to gain a foothold and establish a base of operations to steal data, change info or set up persistent attacks.

Traffic control and filtering for inbound and outbound traffic is critical. Organization should utilize a multilayered approach relying on firewalls, proxies, DMZ perimeter networks and network-based intrusion detection and prevention systems (IDS/IPS). These tools can be used in concert to deny communications with malicious addresses, limit access to trusted ranges at each boundary and look for unusual attacks.

Controls are especially important given the fading boundary lines between internal and external networks. Organizations are increasingly more connected to the internet and to each other. And, the deployment of wireless technologies has further the blurred the internal versus external boundary lines leading some organizations to a 'zero trust' approach for internal and external users. Other organizations achieve effective security deployments relying on carefully configured boundary defenses separating attacks by threat levels, sets of users, data and levels of control. Effective boundary defense helps lower the number of successful attacks allowing you to focus on the attacks that are indeed able to skirt your boundary controls.

Critical findings for boundary defense showed a bad outcome in policy design and operational effectiveness. From a design perspective, we found weaknesses in vulnerability testing processes. And, operationally, the existing (flawed) processes were not followed. Specifically, scheduling was not standardized for vulnerability management processes. And, there were issues in managing changes to configurations of boundary defenses.



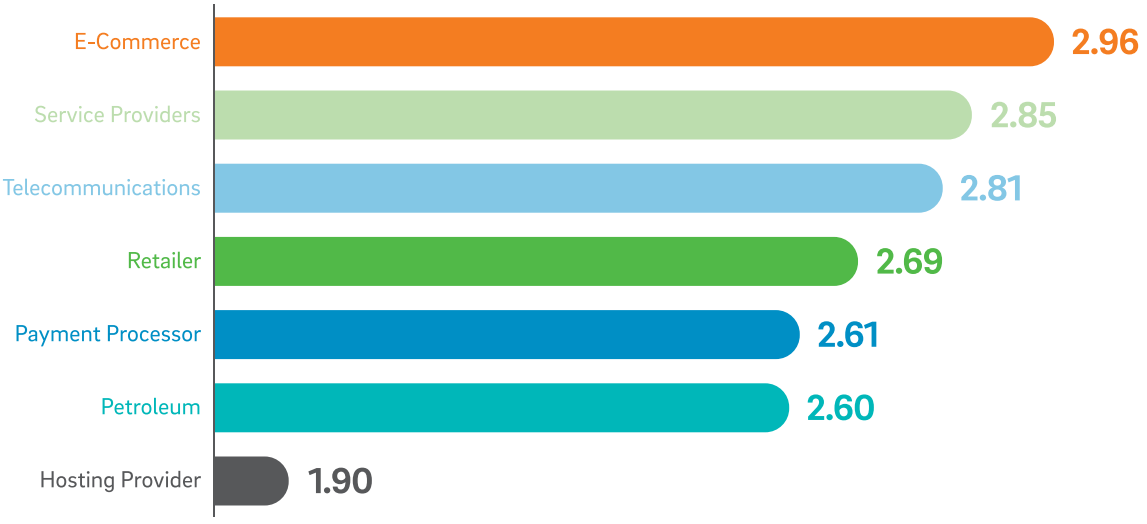
Asset Management

Vulnerable software versions are commonly exploited. And, corrupt websites, documents, files and content may be distributed by attackers using multiple methods including malicious websites or otherwise trustworthy but unknowing host websites. When unsuspecting victims access the content with a vulnerable browser or some other out of date program, adversaries may compromise their machine as a launching point for movement throughout the network or to install keyloggers, sniffers, backdoors or enable long term control with bots and remote-control attacks.

Without appropriate understanding or control of the assets deployed in an organization, protectors can't appropriately secure their assets. Lack of control often leads to users running software they shouldn't need to do their job or by running malware introduced by an attacker after a system compromise. Entities not maintaining asset inventories and classifications for their assets risk being unable to find vulnerable systems or to mitigate attacks.

Managed control and automation is utilized by some organizations to manage documentation of assets and business systems. Application whitelisting may be useful for enforcing execution only by authorized software and to block execution of unauthorized software.

Throughout our assessments, we found configuration management issues and patch management failures. Specifically, we found a lack of consistency for installation of patches across all systems. And, the recommended timeframe for patching often does not match the eventual fix timelines.



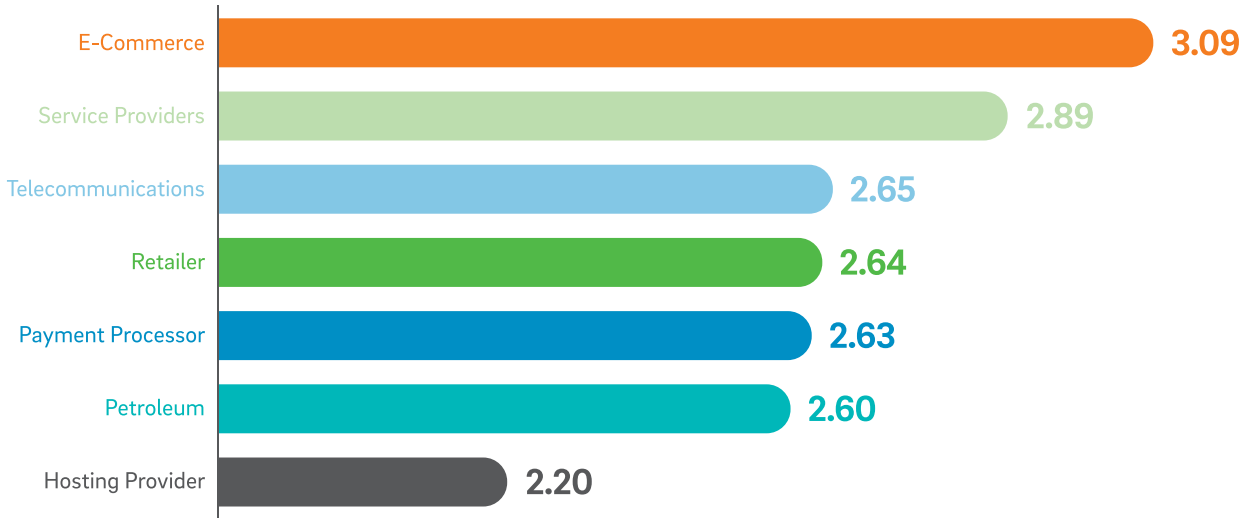
Application Software Security

Coding mistakes, logic errors, incomplete requirements and failures in testing may lead to vulnerabilities in application software. And, organizations may not have the time, knowledge or resources to implement testing for unusual or unexpected conditions.

Information is available to security professionals and hackers alike. The online market for tools and exploit kits is a quality assured and customer centric place to shop, enabling the attackers to find just the right solution they need to attack common vulnerabilities. Examples attacks include buffer overflows, Structured Query Language (SQL) injection, cross-site scripting, cross-site request forgery and click jacking to name a few. Numerous other application vulnerabilities are found all the time.

It's imperative to institute secure coding techniques for the specific coding language and development environments you use. And, best practice is to apply static and dynamic analysis tools to confirm secure coding techniques are being followed.

In our assessments, we found a need for strengthening of secure coding techniques and change management practices. We noted control deficiencies in organizations ensuring that training is up-to-date and that training occurs at an appropriate frequency. We also found a need for greater oversight and consistency in change management processes for application development and security. A major symptom characterizing a lack of oversight and consistency is when changes occur without going through change management processes.



User Management

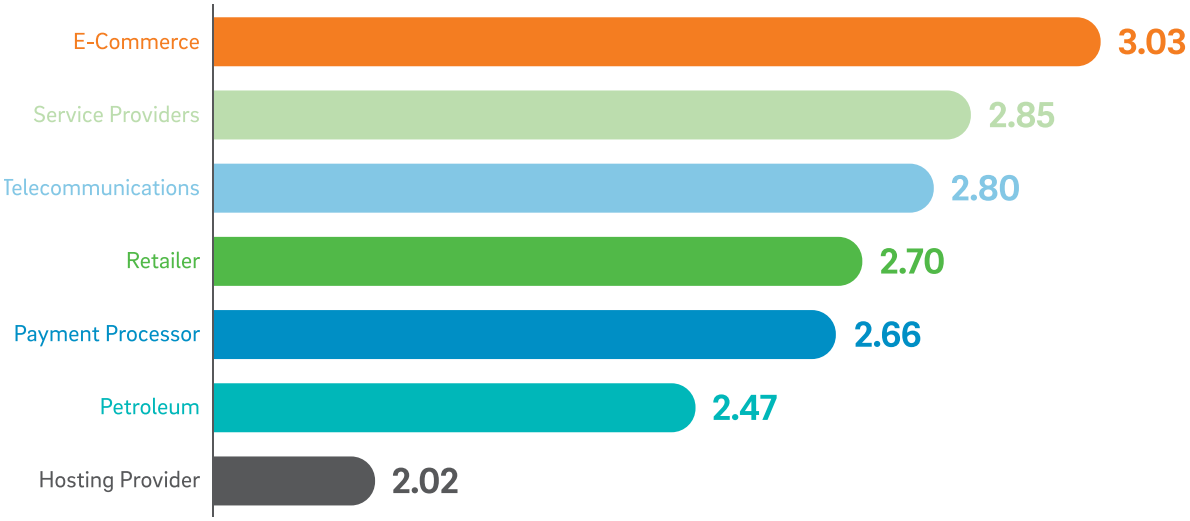
Assailants may exploit legitimate but inactive user accounts or impersonate legitimate users, making the hard task of detection even harder for security professionals. Terminated employee accounts often remain active as do third party vendor accounts or worse vendor accounts with shared credentials. Outside attackers, terminated employees or malicious insiders may get into to abandoned accounts maintaining unauthorized access to systems and sensitive data. And, the misuse (or elevation and abuse) of administrative privileges is especially damaging and a common attack method.

We found many weaknesses in organizations ability to control user access to data, specifically a disregard for providing access only to those with a need to know. Organizations should strengthen processes and periodically conduct an exercise to disable all accounts that cannot be associated with a legitimate business need including a specific process or owner.

All users with administrative access should use a dedicated account only to be used for the specific critical process in question, and not for things like checking email or browsing the internet. System entry logging should be in place and alerting should be configured for any updates, inserts, or deletes from any group with administrative privileges.

Organizations should maintain authentication controls up to and including multifactor authentication (MFA) for privileged access to administrative or critical process functions. Some organizations may choose to implement MFA on all systems regardless of whether systems are managed internally or by an outside party.

Commonly, we found that password and authentication controls were not consistent. And, worse, controls on administrative access are weak. A disturbing finding is the prevalence of generic administrative accounts and the use of shared credentials. If administrative privileges are freely and broadly shared or the same passwords used on multiple systems, it's easier for attackers to gain control quickly or to find multiple paths to ultimately gain unauthorized administrative privileges.



Data Protection

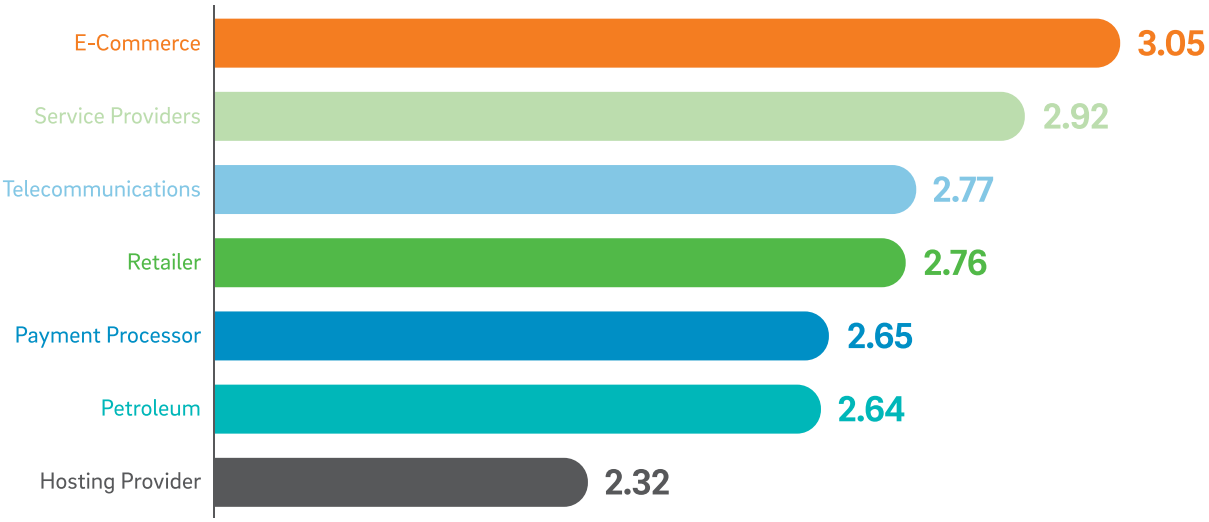
Data exists in many places. Accordingly, the best approach is a one that includes a blend of encryption, data integrity protections and data loss prevention practices. Mobile access and remote servers used to store and process data (i.e. cloud computing) means it's ever more important to fight against data compromise and to limit and report on legitimate data outflows. Some data is leaked and stolen, but most data loss is the consequence of poorly understood data practices, a lack of effective policy and user error. This loss of control of the data in an organization's custody is a major problem.

Many organizations do not accurately identify and isolate their most sensitive data. Nor do they sufficiently separate sensitive assets, from less restricted and public information on their internal networks. In the worst cases, internal users have access to critical data or systems they don't need to do their job. Once inside a poorly segregated network attackers may easily find and steal info, do physical harm or disrupt operations. Companies should segment their network based on the classification of the info stored on their servers, specifically keeping sensitive data on separate virtual local area networks (VLANs).

Data protection in recent years has been marked by a noticeable shift from protecting the network and controlling user access to a current state where the focus is protecting the data itself. DLP is the commonly accepted approach to protecting people process and systems by monitoring and protecting data in use, data in motion and data at rest. Victim organizations often are not aware of data loss because they weren't monitoring normal data flows and watching for illegitimate exfiltration of data. As discussed with Boundary Defense and reiterated here, organizations should use automated tools that protect the boundary by monitoring and alerting, or outright blocking, of unauthorized transmission of sensitive data.

Encryption provides assurance that even if data is lost, it's unfeasible to access in any reasonable amount of time or without significant resources. Note, that doesn't mean you shouldn't have other controls to not lose the data in the first place. Encryption for data in motion and at data at rest is needed. And, the processes for generation, use and destruction of encryption keys should be based on proven processes.

We find weak encryption algorithms in use. Organizations need to stay abreast of the National Institute of Science and Technology (NIST) listing of approved encryption strengths and practices. Review of algorithms and key lengths is recommended on an annual basis. And, the appropriate security controls should be in place for multitenant environments including key management and use of hardware security modules (HSMs).



Security Testing and Monitoring

Information security professionals must navigate a constantly changing landscape and overcome new tasks as a result of changing software releases, patches and new security guidance. Specifically, vulnerability management must be a continual process. Organizations must scan, test, remediate with updates or deploy patches for critical issues and otherwise assess the risk of taking corrective actions or not.

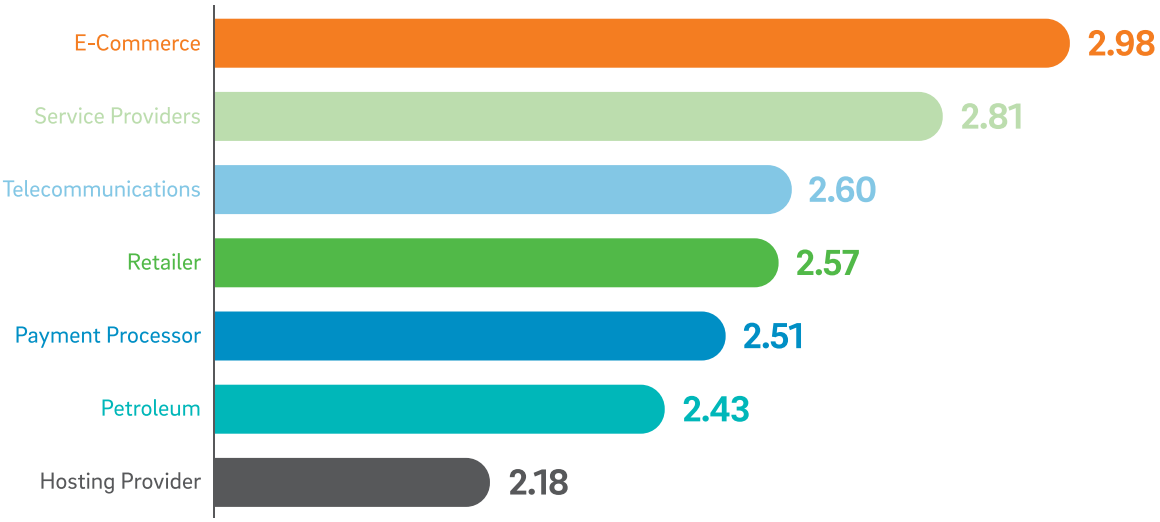
Enterprises face the high likelihood of compromise if they do not maintain a vulnerability management program to preemptively expose and address vulnerabilities. Organizations should use a PCI approved scanning vendor (ASV) tool to automatically scan systems for potential vulnerabilities on at least a weekly basis or more frequently. Entities should set up automated software update tools to make sure all operating systems and programs are using the latest security updates from the vendor.

A mature posture requires a wide-ranging program including policies, governance, technical defenses and proper reaction by real people. Hackers will seek to use the break between the intended protective design and the actual implementation or maintenance of a control. Because technology, vulnerabilities and attack methods are continually changing organizations must conduct periodic tests of their protections to uncover gaps and use penetration testing to figure out whether the gap may be exploited.

Organizations with highly sensitive data or with complex environments, may elect to conduct red team testing to improve organizational readiness, improve training for security professionals and examine current operations. Penetration testing should include a wide range of tests for different attack types applicable to your organization.

In our maturity assessments, we found many issues with vulnerability scanning. In many organizations we noted turnover of employees as a challenge affecting the ability of the entity to maintain security testing. Organizations also report challenges in understanding the changing guidance on vulnerability management by the PCI Security Standards Council (SSC). Specifically, clients expressed not understanding guidance and parameters on what "quarterly" means when seeking four consecutive quarters of passing vulnerability scans.

Incident response management (IRM) processes need to be strengthened, there is lack of training on IRM processes, a general lack of understanding by employees of their roles in the IRM process and organizations suffer from a lack of formalization in their testing process.

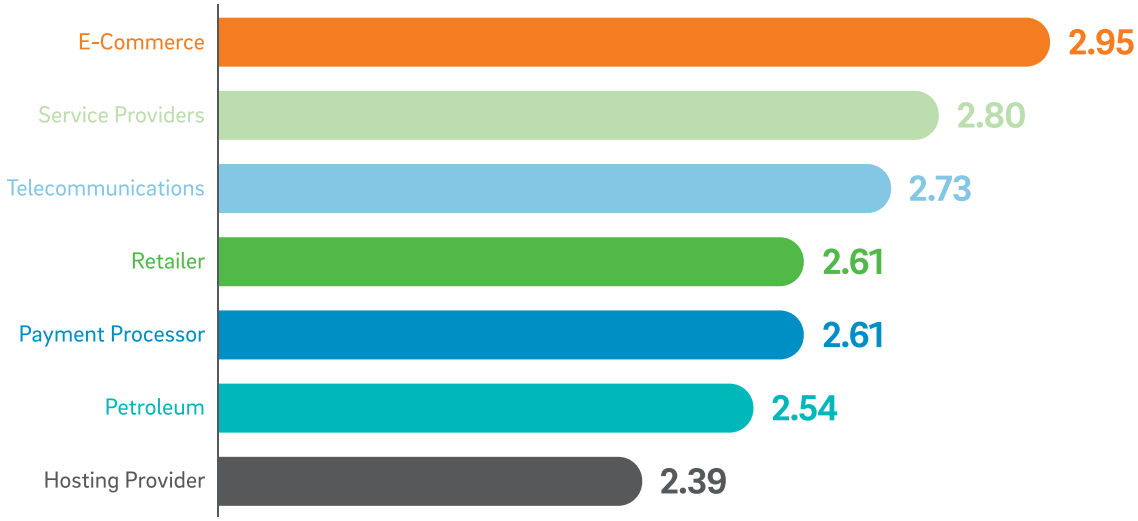


Training

The success or breakdown of an organization depends on people and their action or inaction. People are susceptible to attacks and errors. And, at the same time those people are tasked with important functions for which they may not have complete information. Important functions include system design, implementation, operation and oversight for vast systems, processes and data. Engineers and architects may miss the opportunity to follow secure coding practices. IT professionals may misunderstand the need for security and miss opportunities to maintain IT artifacts and logs and end users may get hooked by a phishing attack. Security pros may not be able to keep up with new and changing info and as a result fail to quantify, and fail to convey to executives, the true importance cybersecurity in the overall mission of the organization. Without quantifying and communicating the impact of training and performance failures organizations have no reasonable way of making appropriate investment decisions.

Organizations should conduct periodic assessments to understand what behaviors employees and connected entities are not performing and use this to build a training program. Each and every employee should be trained on how to identify different forms of social engineering attacks, such as phishing, phone scams and other common attacks. And, secure coding training should be provided to applicable engineers and developers.

In our research, we discovered oversight of training processes needs to be increased. And, in larger more distributed organizations tracking of training needs to be strengthened, whereas we found that there was only meaningful tracking at the individual organization level. In addition to general informational trainings, there is a strong need for training on the specific internal security policies and procedures that are applicable to employees. And, organizations could improve with more formalized security training.



Compliance Intelligence in Your Organization

SecureTrust can help your organization gain Compliance Intelligence, empowering you with information to be used for your strategic advantage. SecureTrust security maturity ratings show you how your organization rates on process maturity for key controls and subprocesses, so you understand where improvements should be made or where investments should be scaled back based on your organizations unique objectives. With anonymized maturity rankings by industry, you gain an objective view of where you stand against competitors and peers in your industry giving you a starting point from which to plan for ongoing process improvement and to align the maturity of your processes with your organization's goals.

Learn More

SecureTrust maturity reports are delivered in conjunction with PCI DSS compliance assessments. To learn more, contact us at www.securetrust.com.

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com