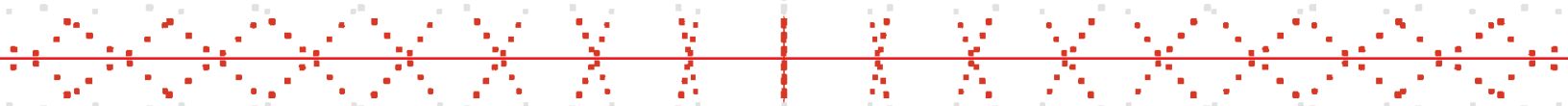
PSR

2020 Payment Security Report

Executive insights



verizon

Verizon has published the Payment Security Report (PSR) since 2010, when we presented the industry with a first-ever study on the actual value and performance of the Payment Card Industry Data Security Standard (PCI DSS). The first and only report of its kind, the PSR provides an in-depth perspective on the regulatory landscape of the payment card industry. Nearly a decade after the first edition, it remains the most anticipated report within the industry that directly addresses the challenges of protecting payment data and meeting compliance requirements.

With every edition, the PSR reveals groundbreaking insights that help shape the industry's understanding of data protection successes and failures, as well as previously undervalued or unknown cause-and-effect factors.

The full report is available at verizon.com/paymentsecurityreport

Verizon's 2019 Payment Security Report—Not Just for PCI

"If you are responsible for cybersecurity or data protection in your organization, stop what you are doing and read this report. Actually, first, go patch your servers and applications, and then read this report. Much like Verizon's Data Breach Investigations Report (DBIR), the Payment Security Report (PSR) is a must-read for security professionals. ... The compliance statistics are informative and show some alarming trends about how well companies are protecting payment card data. Those trends should cause any CISO to look closely at how their organization is handling data protection—and not just for payment cards. ... When I downloaded the PSR, I expected the usual treasure trove of data Verizon usually provides. What delighted me, however, was the report provided a very accessible way to improve security and compliance posture. ... Reading the Verizon report is a good start, but the real value comes from implementing the recommendations. This will ensure greater data protection as well as help with audit compliance."

—Anthony Israel-Davis, Tripwire

Anthony Israel-Davis, "Verizon's 2019 Payment Security Report—Not Just for PCI," The State of Security Blog, Tripwire, Inc., Dec 3, 2019.

www.tripwire.com/state-of-security/regulatory-compliance/verizons-2019-payment-report/

Verizon Payment Security Report history

2010: Complexity and uncertainty

An exploration of the complexity of PCI security, the growing pains of PCI compliance and the need to evolve toward a process-driven approach for compliance

2011: Dealing with evolution

A review of the changing compliance requirements, with insights into the importance of sound decision-making and how organizations can position themselves for success

2014: Simplifying complexity

A review of the value of compliance, the impact of PCI DSS changes, the need for sustainability and how to improve scope reduction and compliance program management

2015: Achieving sustainability

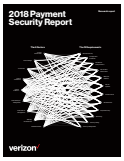
A focused look at improving the sustainability of compliance, and a review of the state of scope reduction and payment security

2016: Developing proficiency

Developing data security proficiency, skills and experience, and applying a structured approach to compliance management

2017: Establishing internal control

The importance of establishing and maintaining an internal control environment and a holistic approach, including security control life-cycle management



2018: Sustainable control effectiveness

Introduction of five practical models to achieve sustainable control effectiveness across your control environment, including the 9 Factors of Control Effectiveness and Sustainability, and the 5 Constraints of Organizational Proficiency

2019: Evaluating program performance

Achieving high-performance security programs with sustainable and effective controls in a predictable manner, and addressing constraints that prevent continuous improvement of process and capability maturity

Data security: Complex but not complicated

Too few organizational leaders, C-suite executives and others understand the underlying reasons for their company's lack of security control sustainability and control effectiveness. For this reason, we devoted the 2020 PSR to the challenges Chief Information Security Officers (CISOs) face in designing, implementing and executing a sound data security compliance program and the power of strategic thinking. We distill a range of security and compliance subjects into valuable insights to help CISOs break down complex ideas into digestible bits. The report explores various tools, tactics and methods applied by numerous organizations, and takes a look at why some companies accomplish so much more than others in their efforts to achieve sustainable and effective data security. We distinguish between approaches that separate busy security teams from productive security teams, the different ways decisions are made that impact how strategies are formed and which goals are embraced. For example, why are technology solutions prioritized while the maturity development of capabilities and processes is ignored? How can leaders adapt, innovate and evolve during challenging times to improve their control environment posture and security cultures? We explain the top security pitfalls and present solutions to equip CISOs with approaches to take with data security compliance challenges. Finally, we explore the essential elements needed to successfully construct and cross the compliance bridge without falling prey to the impact of external environmental shifts during challenging times.

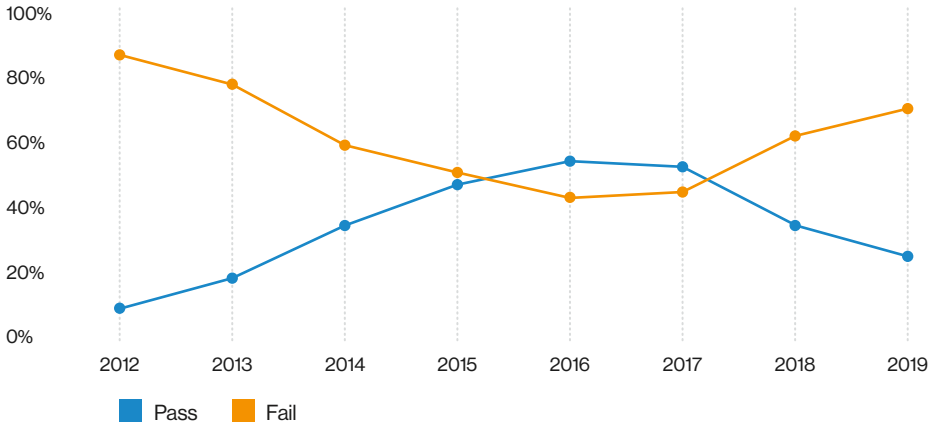
> "One would think that, with the introduction of advanced security technology, increased regulatory focus and incentives for business to invest in the protection of information, security incidents would be rare. However, the truth is that even with the advances being made, security incidents still happen. Private information is still compromised. Internal incidents and fraud are reported all too frequently. Why is information security not improving in leaps and bounds? One answer is that information security professionals continue to find themselves reacting to issues within the enterprise rather than taking a proactive stance. This constant firefighting leaves little time for innovation, strategic thinking and planning. Security professionals revert to applying controls to problems as they arise, often with an overreliance on technology. This is often accompanied by a lack of historical data, so problems continue to occur, even though they have been 'fixed' at some previous point. ...
>
> "Additionally, many enterprise cultures have not accepted information security, and information security managers continue to struggle to demonstrate value. When information risk management is not integrated into the business, organisational silos can reduce opportunities for strategic solutions. A holistic risk-based approach to managing information assets must be implemented."[1]
>
> —Rolf M. von Roessing, "The Business Model for Information Security," ISACA, 2010

1 Rolf M. von Roessing, The Business Model for Information Security, ISACA, 2010. https://www.isaca.org/bookstore/it-governance-and-business-management/wbmis1

State of compliance sustainability

Threats to payment card data continue to increase and impact the payment security landscape in numerous—and increasingly insidious—ways. The negative disruption from data breaches can have a temporary or lasting impact on an organization's sales and company stock price and reputation. With the potential for such severe repercussions, it's difficult to understand why compliance sustainability continues to decline, as seen in our most-recently compiled Verizon data in the Verizon 2020 PSR. Fewer and fewer organizations are demonstrating the ability to keep a minimum baseline of security controls in place. In 2019, from the total population of organizations assessed on PCI DSS compliance within our combined dataset, only 27.9%[2] of organizations achieved 100% compliance during their interim compliance validation. This is a further 8.8 percentage-point (pp) drop from the year before when only 36.7% of organizations demonstrated full compliance. With a nearly 10 pp annual drop in full compliance, we need to focus on organizations developing sustainable compliance.

Figure 1. Sustainability trend



2 For details about the dataset, see the 2020 PSR Methodology section.

The compliance story

Many organizations lack the resources (capacity, capabilities and competence) as well as commitment from business leaders (communication and culture) to support data security and compliance initiatives. Various reasons exist for why organizations don't succeed in addressing such neglect. The reasons given are often superficial and speculative: willful inattention, lack of resources, data security not being treated as a business priority, executive leadership's failure to support the CISO, the steering committee's inability to execute a sound data security compliance strategy, etc. While these reasons may be applicable in some cases, clarification of the root cause and primary contributing factors is essential before organizations select solutions to maximize the business value of data security and compliance. In previous editions of the PSR, we reviewed in detail the concepts of control effectiveness and sustainability. We introduced the 9-5-4 Compliance Program Performance Evaluation Framework[3] (the 9 Factors of Control Effectiveness and Sustainability, the 5 Constraints of Organizational Proficiency and the 4 Lines of Assurance) as a valuable tool to help implement, maintain and measure control effectiveness. In the 2019 PSR, we reviewed how organizations can address constraints and develop data security compliance management proficiencies to become more efficient. We also discussed the application of metrics and maturity models for improving the sustainability and effectiveness of the control environment. What next steps should your organization take?

Payment security threats

According to the 2020 Data Breach Investigations Report (DBIR):[4]

- Retail: 99% of incidents are financially motivated, with payment data and personal credentials continuing to be prized. Web applications, rather than point-of-sale (POS) devices, are now the main cause of retail breaches
- Financial and insurance: 30% of breaches are caused by web application attacks, primarily driven by external actors using stolen credentials to get access to sensitive data stored in the cloud. The move to online services is a key factor
- Healthcare: Basic human error accounts for 31% of healthcare breaches, with external breaches at 51% percent (up from 42% in the 2019 DBIR), slightly more common than insiders at 48% (59% last year). This vertical remains the industry with the highest number of internal bad actors, due to misuse of the access granted to allow them to do their jobs
- Credential theft and social attacks, such as phishing and business email compromises, cause the majority of breaches (over 67%), specifically:
  - 37% of credential theft breaches used stolen or weak credentials
  - 25% involved phishing
  - Human error accounted for 22%

3 Verizon 2019 Payment Security Report, page 9, 2019. https://www.verizon.com/business/resources/reports/payment-security-report/
4 2020 Verizon Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/dbir/

The nature of poor data security performance

Poor performance on compliance assessments isn't a spontaneous act; rather, it's the outcome of a sequence of activities and events based on strategic planning—or lack thereof. Unless the strategy, business models and operating models for security and compliance are improved, it's mostly symptoms that are addressed. A healthy control environment's system output depends on past and current inputs. It's a causal system. Data security is a process that requires long-term attention to strategic initiatives.

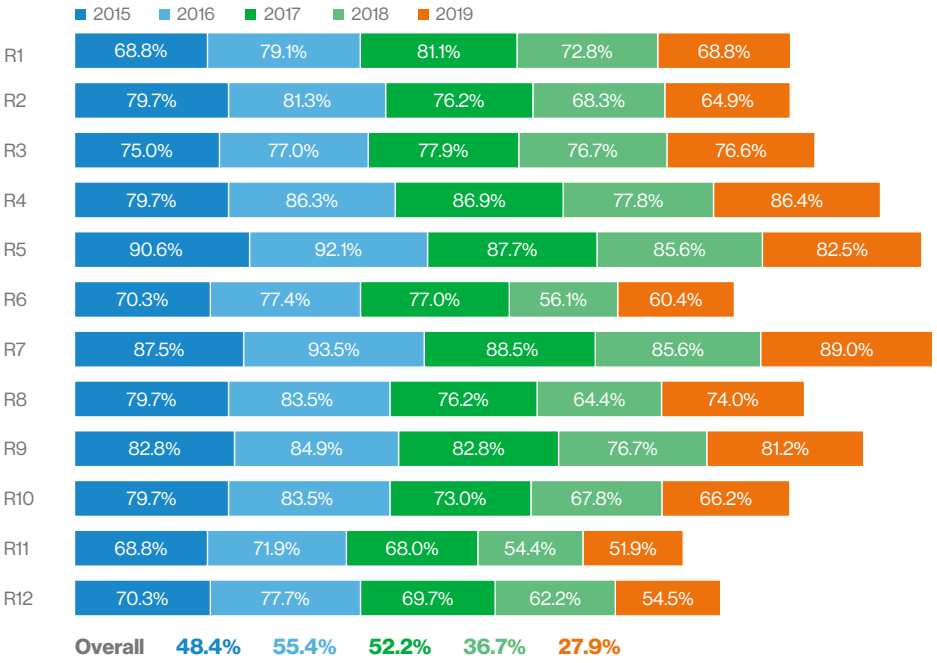
Achieving and maintaining a mature data security compliance program is very seldom solely the result of a standard formula. It is a continuously evolving process in which capabilities and processes are developed over time, where various adjustments (some micro, some macro) are made based on observations at points in time.

You need motivated leadership willing to support a CISO and a steering committee with the means (proficiency) to manage this process. However, this structure is not easy to achieve when the average tenure of a CISO is two years or less! The 2020 PSR delves into CISO challenges and how they contribute to the breakdown of sustainability in control environments.

The report rates control sustainability—the ability to keep controls in place—not the ability to achieve once-per-year compliance. The compliance downturn in 2019 isn't the result of changes to the PCI DSS requirements.[5] A marked decrease in sustainability has been noted by the PSR for several years. There is a substantial drop in full compliance across the Americas region and a substantial increase in control gap, i.e., the percentage of controls found not in place. Asia-Pacific (APAC) is the only region that improved its compliance from the year before. As before, Security testing—Requirement 11—continues to be the requirement that organizations experience the most difficulty with keeping in place.

Five year trends

Figure 2. Full compliance



5 For details on how the PCI DSS requirements changed since the first release of the standard, see the 2020 PSR, Appendix B—the compliance calendar.

Figure 3. Control gap

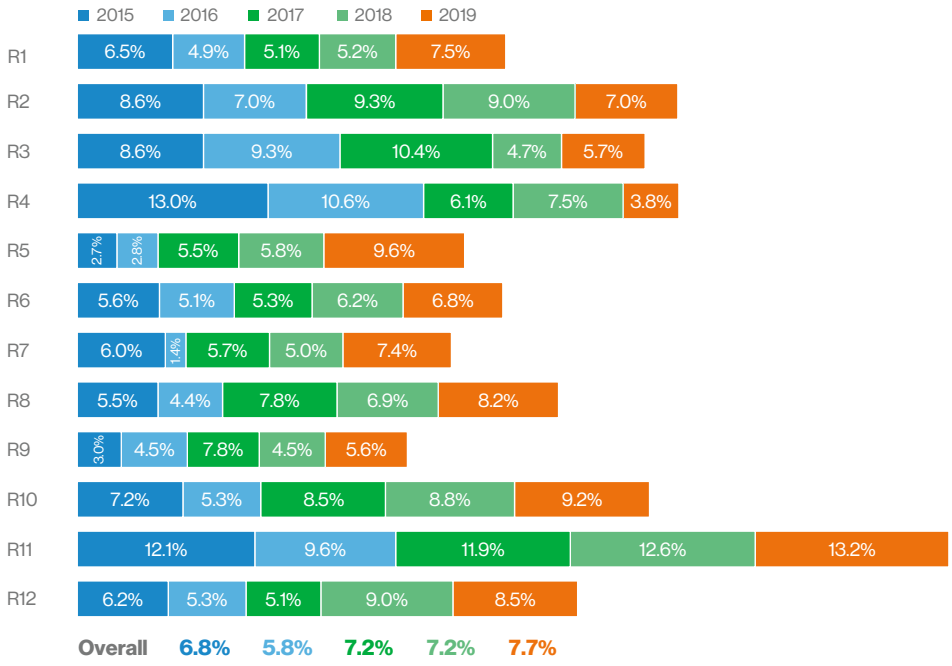
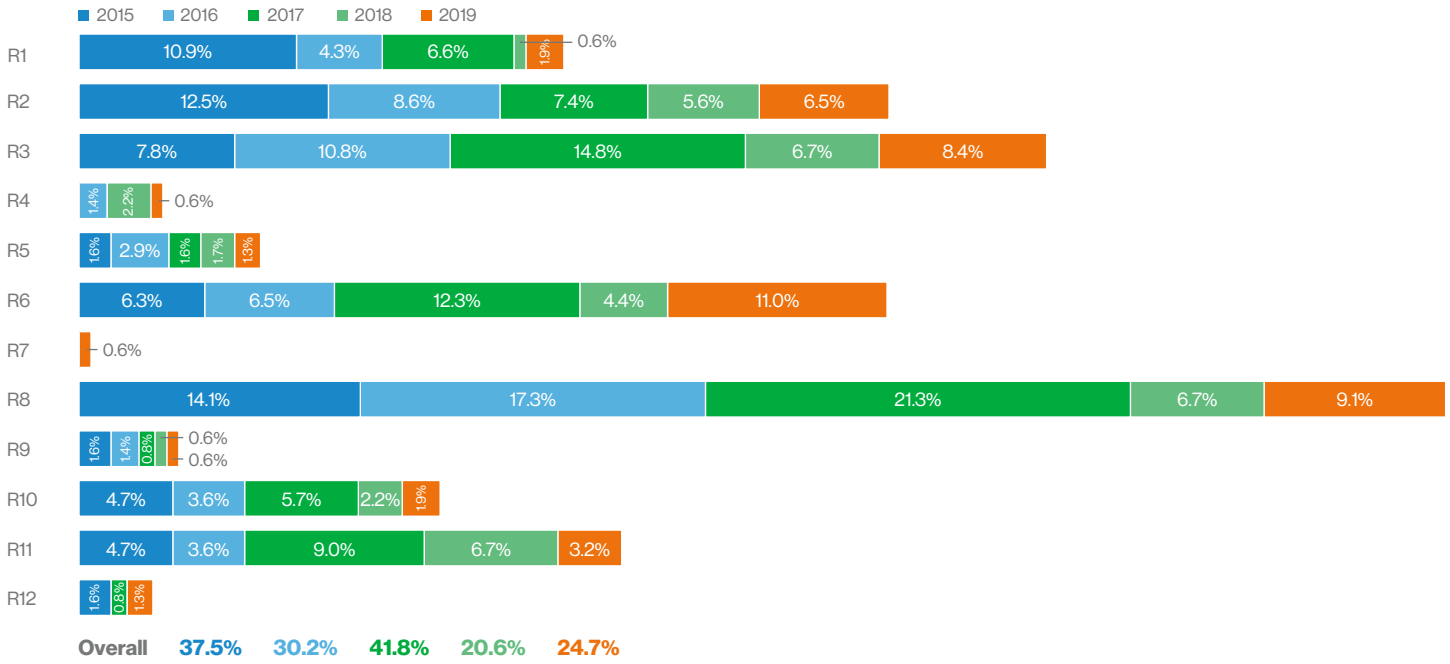


Figure 4. Compensating controls



Top 7 strategic data security management traps

Lack of data security sustainability and effectiveness is largely the result of poor business, strategic and operational architecture design, and execution (see the Commentary section of the 2020 PSR for elaboration on these traps). Addressing these impediments will not only build a strong compliance bridge but also a program that can adapt when necessary.

1. Inadequate leadership

As stated before, data security isn't an IT problem, nor is it one of knowledge. It's a problem of proficiency, where the collective leadership (CEOs, boards of directors, CIOs, CISOs and other executive decision makers) lack the skills, competency, experience and resources to operate effective and sustainable data security compliance management systems.

The first issue is the manner in which organizations approach compliance management and the objectives they prioritize for change. That change needs to be driven from the top—between the CISO, the CIO, the CEO and the board.

Organizations can benefit from reevaluating the role, position and scope of the CISOs' responsibilities and their ability to execute sound security strategies. For starters, most CISOs may be incorrectly positioned in the organization, which is far from ideal, since they often lack the independence and authority to execute programs that are more strategic. Many CISOs are new in their role, due to the high churn rate. In many cases, the compromises they make during their first 100 days in office may haunt them for the rest of their tenure.

2. Failing to secure strategic support

A security strategy and plan includes a prioritized list of objectives with adequate backup for critical role resources. An essential and often missing ingredient for a successful data security strategy is a mutual collaboration, alignment and support between the organization's business objectives and priorities, and its security compliance objectives and priorities. Security strategy is seldom effective without support from a security business model and security operating model. What is missing in many organizations is the communication of the business model for security to the stakeholders. Many security strategies are not supported by a sound security business model that ties the design, strategy and operations to the core processes, which in turn ties the people, processes and technology together. CISOs need to get better at defining the business model to explain to the board how data security and compliance generate value for the organization. This helps to secure needed investments and resources for long-term sustainability. In addition, CISOs must know how to evaluate and improve the strength of security business and operating models. The development of this management skill should be prioritized across the payment security industry by organizations worldwide.

3. Lack of resourcing capabilities

CISOs struggle to get the resources they need to support security strategies. They struggle to address internal constraints. A desperate need exists to address the cybersecurity skills shortage, particularly in the field of security management, and strategic planning and execution. However, the lack of skilled resources isn't the main reason for poor data security sustainability. Developing organizational proficiencies—the skills and experience to address the six primary organizational constraints (capacity, capability, competence, commitment, communication, culture)—is another critical need. Those constraints are preventing organizations from developing the process and capability maturities needed to achieve the primary objective: a sustainable and effective control environment that operates with consistent performance and predictable outputs.

The ultimate goal of PCI security compliance should be to develop and maintain a mature data security compliance program based on a sound strategy that results in sustainable and effective data security with continuous improvement in a consistent and predictable manner.

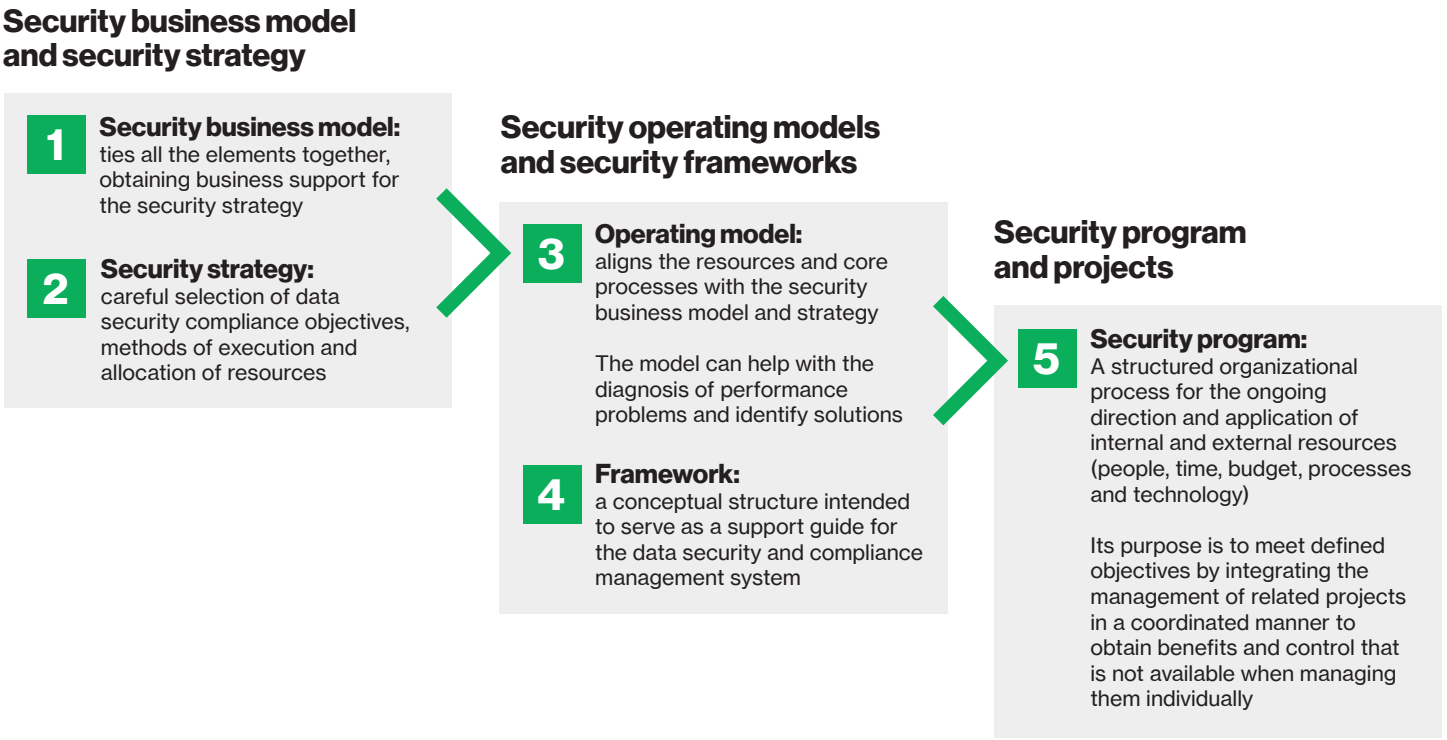
4. Falling short on sound strategic design

Effective data security compliance programs start with a sound strategy. With a poor strategy, whatever cascades down will likely be weak, too. If mature processes and capabilities are not clearly specified objectives in the strategic plan, it's unlikely there will be maturity of data security capabilities. What gets measured gets done. We have covered this important point in many previous PSR publications.

CISOs and business leaders may disagree on security strategies for many reasons, which compromises their ability to achieve support and turn it into meaningful deliverables.

The ultimate goal of PCI security compliance should be to develop and maintain a mature data security compliance program based on a sound strategy that results in sustainable and effective data security with continuous improvement in a consistent and predictable manner. CISOs and their executive teams need to be aware of and align on the most successful strategies others in their industry are using to overcome obstacles for achieving this goal. No need to reinvent the wheel, but it needs shaping to fit. Security strategy design and execution should be supported by industry-accepted security models and frameworks. Such frameworks are only truly effective when applied in alignment with an organization's operational and business objectives.

Figure 5. Aligning security and business operating models



5. Deficient strategy execution

CISO priorities and solutions are far too technology focused. CISOs need to spend a lot more time on processes and strategy to achieve a balance between strategic planning and execution, and managing the day-to-day operational challenges (i.e., "firefighting"). The correct selection, application and adherence to supporting frameworks is the other major piece of the puzzle that organizations get wrong. Some CISOs continue to take shortcuts, many times out of a perceived necessity, at other times because they don't know any better or simply because it's less challenging. They may have to make very difficult compromises on their strategy because funding isn't made available, budgets are cut or security projects and programs are rejected in preference for IT projects. Technology solutions may be sought because a personnel resourcing budget isn't available. While the business will approve a budget for a kit or tool (perceived as a one-off investment), it won't approve a budget for resources requiring an ongoing cost.

When security frameworks are selectively and partially followed, the value of those frameworks is diminished substantially. Taking such shortcuts is prevalent throughout the industry, and many organizations are fairly blatant and blasé about adhering to frameworks. It's essential that CISOs get the requirements of the control environment right first before they execute the program and related projects. Nearly all security incidents can be traced back to poor decisions made during the design and execution of the security strategy and the operational architecture of the control environment.

6. Low capability and process maturity with lack of continuous improvement

We've known for decades that organizations need to develop maturity for data security operations and performance to become consistent and outcomes predictable. PCI DSS, as a baseline compliance standard that establishes minimum levels of assurance, needs to evolve further. Many organizations demonstrate that moving beyond the baseline security standards to deliver enhanced sustainability and maturity—established by frameworks such as the PCI DSS—can be achieved with or without the use of additional standards and frameworks. The achievement of mature data security control environments is in reach of all organizations. What is needed is increased focus on maturing all core processes—instead of the widespread continued focus and over-reliance on technology.

7. Communication and culture constraints

How companies communicate about complex planning projects, such as a compliance program implementation, can impact the likelihood of a breach. Poor company communication can be a significant, underlying reason for why company data compliance is trending downward. CISOs and their teams struggle to communicate and collaborate with the executive team, hampered in part by limited interactions and relationships at the executive level.

Business leaders often fail to see the value of investing time and resources into understanding data security and compliance beyond its more traditional functions. They may remain comfortably involved in supporting other technology areas while believing that compliance with a baseline standard equals security. An important step in developing a broader security culture is having strong communications plans that clarify and justify risk and security in ways that catalyze employees to embrace them. Communication plans that don't directly align with business goals and vision seldom receive the support required to be effective and sustainable across the lifetime of the security strategy execution.

The CISO merry-go-round: Breaking the vicious cycle

Some of the greatest challenges CISOs face relate to securing investments for data security and compliance programs. Investments are needed to realize their security strategy and deliver continuous process and capability improvement. The effort required to secure these funds can result in CISO stress, overwork and tenures of two years or less. This can turn into a slippery slope. Security leaders unable to achieve effective and sustainable control environments leave an organization prematurely, likely breaking any momentum gained on the delivery of a data security management program. It plunges the next CISO into an environment where they, again, are forced to focus on realizing quick wins, which in most cases is technology focused—with projects that drive strategic objectives ending up on the back burner.

In this vicious cycle, organizations don't sufficiently develop their core data security processes and capabilities and, in turn, can't address the six constraints of organizational proficiency. They stay in a reactive mode, responding to events. The balance between strategy and operations can't be achieved. In this cycle, both the CISOs and their teams constantly firefight, and the business leaders don't see the expected security investment return.

One way for CISOs to get off the merry-go-round and break the cycle is to implement and maintain a high-performance data security environment, which is comprised of five key elements. See the 2020 PSR for more details on these elements.[6]

Elements of a high-performance data security environment

The five elements that make up a high-performance data security compliance management environment are:

1. **Security business model (SBM):**

   An overarching model that ties all the elements together to obtain business support for security strategy. This model defines the objectives and how core processes are structured to deliver maximum value—and supports how the organization's models, frameworks and programs are aligned.

2. **Security strategy:**

   The security business model is then translated into a strategy. The strategy is mainly concerned with determining the careful selection and prioritization of the security and compliance approach and objectives, and ultimately guides the allocation of scarce resources. The security strategy must be aligned with a business model. It won't define the "how to." Today, only a small number of CISOs are successful in aligning the cybersecurity function with their organizational strategy.

3. **Security operating model (SOM):**

   The strategy is supported by the security operating model, and concerned with the alignment of resources and processes. The operating model represents how value is created by an organization—and by whom within the organization. The operating model must be aligned with your strategy, or there will be poor execution and an uphill battle to deliver results.

4. **Security frameworks:**

   CISOs are finding it difficult to align their security frameworks with the organization's mission. The correct selection and application of frameworks should move organizations away from being too technically focused.

   Frameworks provide structure. They can be thought of as the skeletal system upon which the body of a sound program can be built. Generally, frameworks are operational in nature and provide a detailed description of how to implement, create or manage a program or process. Frameworks are typically principles-based and open to continuous improvement. As a result, frameworks usually rely on subsidiary standards to "make it happen." The Business Model for Information Security addresses these challenges by offering a way for enterprises to synthesize the frameworks and standards they are utilizing, as well as a formal model they can follow to create a holistic information security program that does more for the enterprise than traditional approaches.[7]

6 Verizon 2019 Payment Security Report, page 10, 2019. https://www.verizon.com/business/resources/reports/payment-security-report/
7 The Business Model for Information Security, ISACA, 2010. https://www.isaca.org/bookstore/it-governance-and-business-management/wbmis1

5. **Security programs and projects:**

   The operating model is supported by the security program. The program delivers outcomes by managing a collection of projects, where the achievement of long-term objectives can only be realized when it's collectively managed as a program. Organizations can incorporate the 9-5-4 framework to evaluate program performance, and to drive process and capability maturity. Program management benefits include improvement of performance among participating projects through integration, alignment of objectives, economies of scale and broad oversight.

   For many organizations, a large part of the journey in PCI security and compliance is about moving from a disjointed set of activities to creating a formalized program. The question of strategy gets to the heart of what it takes to move a program forward. Instead of short-term projects with small, immediate goals, security must evolve into a long-term program with a mission, objectives and strategy that improve the security posture of the organization.[8]

From a governance perspective, there are six major outcomes that the security program should work to achieve.[9] In its publication on information security governance, ISACA defined these outcomes as:

- Strategic alignment
- Risk management
- Value delivery
- Resource management
- Performance management
- Assurance process integration

The intent of a data security compliance management program is to design and execute a governance framework and maintain control over the program activities for extended periods of time. This provides the best possible chance to succeed in achieving the stated objectives with the available resources.

Do not neglect the fundamental principles.

A majority of organizations are still ignoring the cornerstones of a successful data security compliance program. There is immense value in understanding these fundamental building blocks:

The 7 data security principles:

1. Success is achieved by design, not luck
2. All controls must be effective, not just present
3. Controls have dependencies and function with control systems, not in isolation
4. For controls to be sustainable, their control environment must also be sustainable
5. Operating performance indicators should be measured and reported
6. The input, activity and output of all core processes must be consistent and predictable to support timely detection, prevention and correction of performance deviations
7. Continuous improvement must be made toward adequate process and capability maturity

8 Verizon 2019 Payment Security Report, pages 15 to 20, 2019. https://www.verizon.com/business/resources/reports/payment-security-report/

9 The Business Model for Information Security, ISACA, 2010. https://www.isaca.org/bookstore/it-governance-and-business-management/wbmis1
Also, Information Security Governance: Guidance for Information Security Managers, ISACA, 2008. https://www.isaca.org/bookstore/it-governance-and-business-management/w3itg
Also see Board Briefing on IT Governance, 2nd Edition, IT Governance Institute, 2003. https://www.oecd.org/site/ictworkshops/year/2006/37599342.pdf

Verizon 2020 Payment Security Report

Published October 6, 2020

Editorial team

Lead author

Ciske van Oosten

Co-authors

Anne Turner, Cynthia B. Hanson, Dyana Pearson, Dennis Merenguelli, Sky Hackett

Data analysts

Anne Turner, Dyana Pearson, Ron Tosto, Suzanne Widup, Sky Hackett

Contributors

Emmanuel Baeyens, Franklin Tallah, David Kennedy, Rafeeq Rehman, John Galt, Halli Goodman, Jyri Ryhanen, Loic Breat

Content editor

Cynthia B. Hanson

Co-editors

Anne Turner, Dyana Pearson, Sky Hackett, Rein van Koten, Suzanne Widup

Security assurance practice

PCI and Payment Security consulting practice

Global lead: Sean Sweeney

PCI security practice managers

APAC region: Sebastien Mazas

Americas region: Franklin Tallah

EMEA region: Gabriel Leperlier

Global intelligence: Ciske van Oosten

Team email

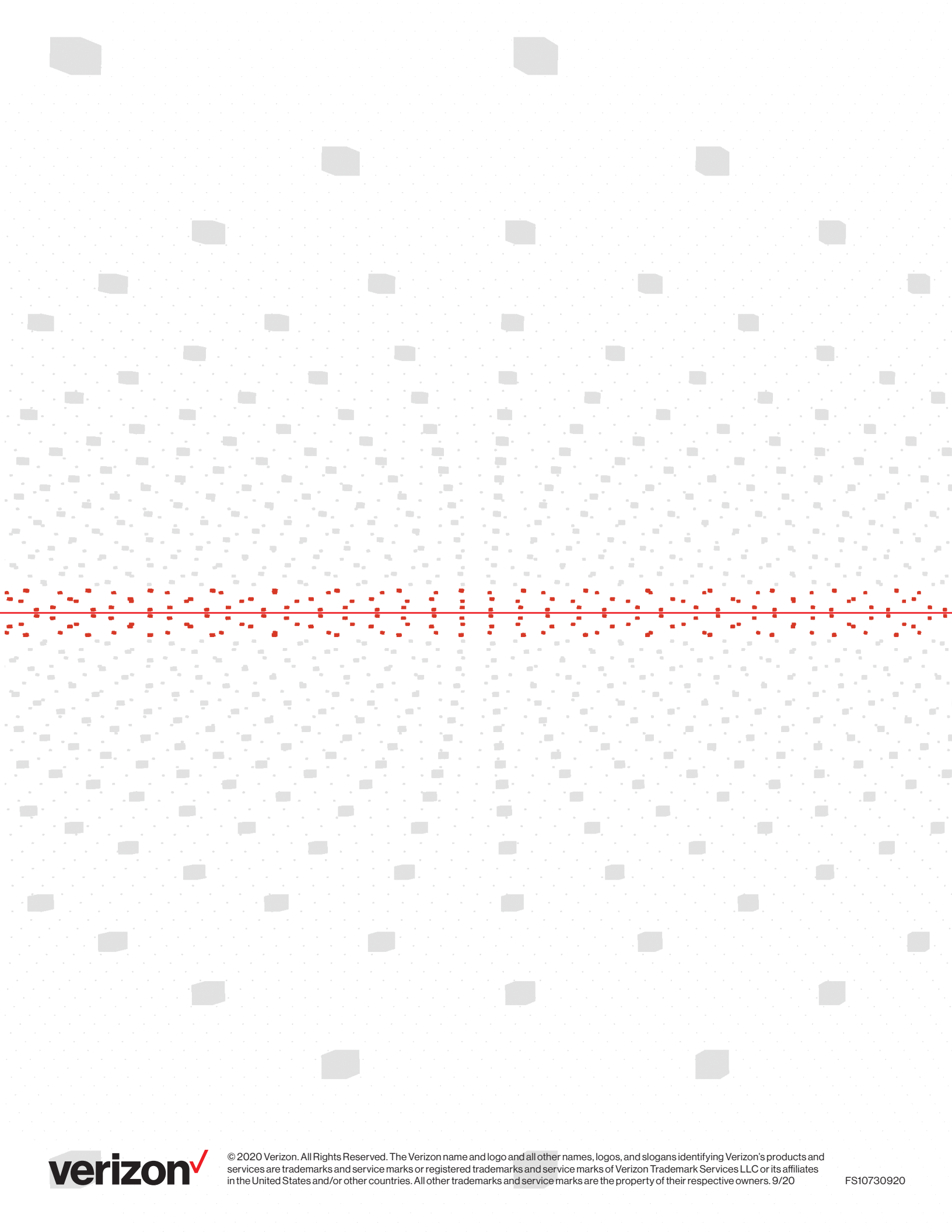
paymentsecurity@verizon.com

PCI DSS data contributors[10]

Third-party contributors

The Advantio Team, Dustin Rich (A-Lign), Héctor Guillermo Martínez, Alberto España, Rogelio Nova, Russell M. Latimer (GMSectec), Anthony Petruso, Michael Vitolo (MegaPlanIT), Jacob Ansari (Schellman)

10 Names, logos, and brands are the property of their respective owners and used for identification purposes only. Use of these names, logos, and brands does not imply endorsement.



FS10730920