The Top Nine factors for Effective Data Protection Controls

What, Why & How

*Lessons from Payment Security Report*

Ciske van Oosten
Senior Manager Global Business Intelligence
June 11th, 2019
Questions

What are Breached and non-Breached companies doing differently?

What can you learn from studying 12 years of data breach investigation data, and correlate that with 11 years of PCI Security compliance data?

How do you determine the effectiveness and sustainability of your control environment?
Differences...

What do breached organizations do differently from non-breached organizations:

1. Prior to being breached
2. During a breach
3. After a breach

**Prior to being breached:** differences in data handling and protection practices, policies, procedures

**During a breach:** differences in the initial reaction to the breach, the ability to respond to the breach, the breach, ability to contain the breach.

**After a breach:** differences in breach recovery and data protection posture improvement
Why Do Organizations Get Breached And Data Compromised?

Security breaches and data compromises occur because one or more controls are:

a. missing (not implemented), or
b. not fully operational (partially implemented), or
c. operating as designed, but is knowingly or unknowingly ineffective, or
d. a control was operated in violation of its design specifications.

The real question is: Why did a/b/c/d occur?

*WHAT you protect, WHERE and WHEN you protect it is important.*
*But understanding HOW you do it, is essential.*

It’s not a knowledge or technology problem.

It’s a proficiency problem.
Operational Risk

Four broad operational risk categories:

1. **Actions of people**: Action, or lack of action, taken by people either deliberately or accidentally that impact security.

2. **Systems and technology failures**: Failure of hardware, software and information systems.

3. **Failed internal processes**: Problems in internal business processes that impact the ability to implement, manage and sustain security.

4. **External events**: Issues beyond the control of the company (disasters, legal issues and service provider dependencies).

---

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Involuntary &amp; Malicious</td>
<td>2.1 Hardware</td>
<td>3.1 Process design or execution</td>
<td>4.1 Disasters</td>
</tr>
<tr>
<td>1.2 Errors</td>
<td>2.1.1 Capacity</td>
<td>3.1.1 Process flow</td>
<td>4.1.1 Weather event</td>
</tr>
<tr>
<td>1.3 Omissions</td>
<td>2.1.2 Performance</td>
<td>3.1.2 Process documentation</td>
<td>4.1.2 Fire</td>
</tr>
<tr>
<td>2.1.3 Maintenance</td>
<td>3.1.3 Roles and responsibilities</td>
<td>4.1.3 Flood</td>
<td></td>
</tr>
<tr>
<td>2.1.4 Obsolescence</td>
<td>3.1.4 Notifications and alerts</td>
<td>4.1.4 Earthquake</td>
<td></td>
</tr>
<tr>
<td>3.1.5 Failures</td>
<td>3.1.6 Information flow</td>
<td>4.1.5 Unaided</td>
<td></td>
</tr>
<tr>
<td>3.1.6 Incidents</td>
<td>3.1.7 Violations</td>
<td>4.1.6 Pandemic</td>
<td></td>
</tr>
<tr>
<td>3.1.7 Incidents</td>
<td>3.1.8 Insider threats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2 External events</td>
<td>3.1.9 External threats</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.
The landscape today...

- The majority of breaches are committed by threat actors that exploit known vulnerabilities, using attacks that are not considered to be highly sophisticated.

- In the majority of data breach cases, the weaknesses that were exploited could have been prevented by applying fundamental principles of data protection. For example:
  - **Devaluing the data** – using encryption or tokenization for example.
  - **System hardening** – exploits could have been prevented applying available security patches for known vulnerabilities. Is it not true that in many data breach cases system patches were available for more than 12 months at the time of the breach?
  - **Strong authentication** – implementing strong multi-factor authentication to prevent access to data and egress of data.

Given the above, can it be claimed today that most data compromise occur as result of the organization’s inability to address organizational complexity, or is it a consistent, widespread failure to attend to fundamental data protection principles, or both?
COMPLEXITY
Infographic:

The role of a CISO

Source: Louis Botha
The Payment Security Report
Payment Security Report

A “go to” industry resource for the past nine years. The first and only industry research report of its kind to provide a global perspective on the state of payment security.

2010: Complexity and uncertainty
An exploration of the complexity of PCI security, the growing pains of the PCI compliance regulation, 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 and impact of PCI DSS standard changes, the need for sustainability, how to improve scope reduction and compliance program management.

2015: Achieving sustainability
A focus on improving the sustainability of compliance, a review of the state of scope reduction, payment security innovation and the need to avoid over-reliance on technology.

2016: Developing proficiency
The need to develop data protection proficiency, necessary skills and experience.

2017: Establishing internal control
The importance of establishing and maintaining an internal control environment and a holistic approach, including security control lifecycle management.
Verizon 2018 Payment Security Report

Figure 23: Distribution of IoT data by region

Europe 23%
Asia Pacific 20%
North America 45%

Figure 24: Distribution of IoT data by industry

Financial Services 50%
Hospitality 11%
Retail 12%
IT Services 15%
Data Protection Sustainability

The Verizon PSR is the only industry report that tracks data protection sustainability using PCI Data Security as a barometer to measure data protection performance of organizations worldwide.

Worldwide, the top performing industry remains IT services, where over three-quarters of organizations (77.8%) achieved full compliance. Retail (56.3%) and financial services (47.9%) were significantly ahead of hospitality organizations (38.5%) which demonstrated the lowest compliance sustainability.

Raising awareness about the importance of actively managing an organization’s control environment effectively; nearly half (47.5%) of the organizations Verizon assessed during interim PCI DSS compliance validation did not maintain all DSS controls.

The majority of organizations across the payment security industry have room for improvement in designing and maintaining sustainable control environments. Trying to address the sustainability problem by attempting to improve it at an individual control level is unlikely to succeed. Control sustainability must start with improving the maturity of the control environment and follow with regular performance measurement.
Control environment management issues

- **52%** of organizations do NOT map security control dependencies.
- **30%** of organizations use some form of documented control design profile for security controls.
- **70%** of organizations have no control-to-risk mapping documentation.

- **34%** of organizations do not use any metrics to measure and track the performance of their controls (apart from compliance validation reporting).
- **45%** of organizations rate the maturity of their security program as “Operational and Managed”. Only 20% rate it as “Advanced”.
- **18%** of organizations (less than a quarter) measure their PCI DSS controls more frequently than what the PCI DSS requires, across their entire environment.

*Source: Verizon 2018 Payment Security Report Global PCI DSS Program Management Mini-Survey*
Global Industry Problems

An inability to predict the outcomes of their data protection and compliance programs - due to lack of capability maturity in performance measurement and other competencies.

Sustainability Problem:

- Nearly half (47.5%) of the organizations Verizon assessed for interim PCI DSS compliance validation had not maintained all DSS controls.

Standards and Frameworks:

- About a quarter of organizations (22%) do not follow a unified compliance approach, and have no plans to do so in the future either.
- About two-thirds of organizations (66%) use more than one industry standard framework in addition to PCI DSS.
- About half of organizations (48%) follow a unified compliance approach to meet requirements from multiple standards.
- About half of organizations (50%) have PCI DSS compliance programs that are not part of a larger GRC program.

Measurement and Reporting:

- In terms of compliance reporting, two fifths (40%) only measure their PCI compliance annually for compliance validation purposes. Less than a quarter (19%) measure and report their PCI DSS compliance monthly.

The shortcomings of PCI Data Security compliance

While PCI DSS guidance documents promote risk management and sustainability of controls, none of the versions of PCI DSS to date mandates measurement and reporting of:

- The condition and effectiveness of the control environment
- Individual security control effectiveness
  - Control systems and control dependencies
  - Control risk, control robustness and control resilience
  - Control design
- Control lifecycle management
- Compliance performance management
- Control maturity measurement
The Top 9 Factors

1. Control Environment
2. Control Design
3. Control Risk
4. Control Robustness
5. Control Resilience
6. Control Lifecycle Management
7. Performance Management
8. Maturity Measurement
9. Self-Assessment
Valuable Security Books

1. CISO Guidance
2. Program Management
3. General Security Principles and Management
4. Risk Assessment & Management
5. Security Controls & Frameworks
# Books: CISO Guidance

<table>
<thead>
<tr>
<th>YEAR</th>
<th>TITLE</th>
<th>AUTHOR</th>
<th>PUBLISHER</th>
<th>PAGES</th>
<th>ISBN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Establishing and Managing an Information Protection Program</td>
<td></td>
<td>Heinemann</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1st Edition</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>Data Protection and Information Lifecycle Management</td>
<td>Tom Petrocelli</td>
<td>Prentice hall</td>
<td>288</td>
<td>9780131927575</td>
</tr>
<tr>
<td>2013</td>
<td>CISO and Now What?</td>
<td>Michael Oberlaender</td>
<td>Createspace</td>
<td>102</td>
<td>9781480237414</td>
</tr>
<tr>
<td>2013</td>
<td>Executive’s Guide to COSO Internal Controls: Understanding and</td>
<td>Robert Moeller</td>
<td>Wiley</td>
<td>304</td>
<td>9781118626412</td>
</tr>
<tr>
<td></td>
<td>Implementing the New Framework</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>Enterprise Cybersecurity: How to Build a Successful Cyberdefense</td>
<td>Scott Donaldson, Stanley</td>
<td>Apress</td>
<td>536</td>
<td>9781430260820</td>
</tr>
<tr>
<td></td>
<td>Program Against Advanced Threats</td>
<td>Siegel, Chris Williams,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Abdu Aslam</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matt Stamper</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Books: Program Management

<table>
<thead>
<tr>
<th>YEAR</th>
<th>TITLE</th>
<th>AUTHOR</th>
<th>PUBLISHER</th>
<th>PAGES</th>
<th>ISBN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Implementing Program Management: Templates and Forms Aligned with the Standard for Program Management and Other Best Practices 3rd Edition</td>
<td>Ginger Levin, Allen R. Green</td>
<td>Auerbach</td>
<td>328</td>
<td>9781466597716</td>
</tr>
<tr>
<td>2017</td>
<td>The Standard for Program Management Fourth edition</td>
<td>Project Management Institute</td>
<td>Project Management Institute</td>
<td>176</td>
<td>9781628251968</td>
</tr>
<tr>
<td>2018</td>
<td>Program Management: A Practical Guide</td>
<td>Sorin Dumitrascu</td>
<td>Independent</td>
<td>621</td>
<td>9781976928581</td>
</tr>
</tbody>
</table>
# Books: General Security Principles & Management

<table>
<thead>
<tr>
<th>YEAR</th>
<th>TITLE</th>
<th>AUTHOR</th>
<th>PUBLISHER</th>
<th>PAGES</th>
<th>ISBN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Principles and Practice of Information Security</td>
<td>Linda Volonino &amp; Stephen Robinson</td>
<td>Pearson</td>
<td>256</td>
<td>9780131840270</td>
</tr>
<tr>
<td>3</td>
<td>Executive Guide to Information Security: Threats, Challenges, and Solutions</td>
<td>Mark Egan, Tim Mather</td>
<td>Addison-Wesley</td>
<td>288</td>
<td>9780321304513</td>
</tr>
<tr>
<td>4</td>
<td>Beautiful Security: Leading Security Experts Explain How They Think</td>
<td>Andy Oram, John Viega</td>
<td>O'Reilly Media</td>
<td>304</td>
<td>9780596527488</td>
</tr>
<tr>
<td>5</td>
<td>Psychology of Information Security: Resolving Conflicts Between Security Compliance and Human Behaviour</td>
<td>Leron Zinatullin</td>
<td>IT Governance Ltd</td>
<td>128</td>
<td>9781849287890</td>
</tr>
</tbody>
</table>
# Books: Risk Assessment & Management

<table>
<thead>
<tr>
<th>YEAR</th>
<th>TITLE</th>
<th>AUTHOR</th>
<th>PUBLISHER</th>
<th>PAGES</th>
<th>ISBN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Risk Management for Security Professionals</td>
<td>Carl A. Roper</td>
<td>Butterworth-Heinemann</td>
<td>304</td>
<td>9780750671132</td>
</tr>
<tr>
<td>2</td>
<td>Information Security Risk Analysis</td>
<td>Thomas R. Peltier</td>
<td>Auerbach</td>
<td>281</td>
<td>9780849308802</td>
</tr>
<tr>
<td>3</td>
<td>Managing Information Security Risks: The OCTAVE</td>
<td>Christopher Alberts &amp; Audrey Dorofee</td>
<td>Addison-Wesley</td>
<td>512</td>
<td>9780321118868</td>
</tr>
<tr>
<td>5</td>
<td>A Practical Guide to Security Assessments</td>
<td>Sudhanshu Kairab</td>
<td>Auerbach</td>
<td>498</td>
<td>9780849317064</td>
</tr>
<tr>
<td>6</td>
<td>The Failure of Risk Management: Why It's Broken and How to Fix It</td>
<td>Douglas W. Hubbard</td>
<td>Wiley</td>
<td>281</td>
<td>9780470387955</td>
</tr>
<tr>
<td>8</td>
<td>Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis</td>
<td>Mark Talabis &amp; Jason Martin</td>
<td>Syngress</td>
<td>258</td>
<td>9781597497350</td>
</tr>
<tr>
<td>10</td>
<td>IT Security Risk Control Management: An Audit Preparation Plan</td>
<td>Raymond Pompon</td>
<td>Apress</td>
<td>311</td>
<td>9781484221396</td>
</tr>
</tbody>
</table>
## Books: Security Controls & Frameworks

<table>
<thead>
<tr>
<th>YEAR</th>
<th>TITLE</th>
<th>AUTHOR</th>
<th>PUBLISHER</th>
<th>PAGES</th>
<th>ISBN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Executive's Guide to COSO Internal Controls: Understanding and Implementing the New Framework</td>
<td>Robert Moeller</td>
<td>Wiley</td>
<td>304</td>
<td>9781118626412</td>
</tr>
<tr>
<td>2016</td>
<td>Security Controls Evaluation, Testing, and Assessment Handbook</td>
<td>Leighton Johnson</td>
<td>Syngress</td>
<td>678</td>
<td>9780128023242</td>
</tr>
</tbody>
</table>
## Books: Security Measurement & Metrics

<table>
<thead>
<tr>
<th>YEAR</th>
<th>TITLE</th>
<th>AUTHOR</th>
<th>PUBLISHER</th>
<th>PAGES</th>
<th>ISBN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Chief Information Security Officer's Toolkit: Security Program Metrics</td>
<td>Fred Cohen</td>
<td>Fred Cohen &amp; Associates</td>
<td>228</td>
<td>9781878109354</td>
</tr>
<tr>
<td>2</td>
<td>Security Metrics: Replacing Fear, Uncertainty, and Doubt</td>
<td>Andrew Jaquith</td>
<td>Addison-Wesley</td>
<td>336</td>
<td>9780321349989</td>
</tr>
<tr>
<td>3</td>
<td>How to Measure Anything: Finding the Value of &quot;Intangibles&quot; in Business</td>
<td>Douglas Hubbard</td>
<td>John Wiley</td>
<td>287</td>
<td>9780470110126</td>
</tr>
<tr>
<td>4</td>
<td>Complete Guide to Security and Privacy Metrics - Measuring regulatory compliance, operational resilience, and ROI</td>
<td>Debra S. Herrmann</td>
<td>Auerbach</td>
<td>824</td>
<td>9780849354021</td>
</tr>
<tr>
<td>7</td>
<td>Pragmatic Information Security Metrics</td>
<td>W. Krag Brotby &amp; Gary Hinson</td>
<td>Auerbach</td>
<td>512</td>
<td>9781439881521</td>
</tr>
<tr>
<td>8</td>
<td>Measures and Metrics in Corporate Security</td>
<td>George Campbell</td>
<td>Elsevier</td>
<td>145</td>
<td>9780128006887</td>
</tr>
<tr>
<td>10</td>
<td>How to Measure Anything in Cybersecurity Risk</td>
<td>Douglas Hubbard, &amp; Richard Seiersen</td>
<td>Wiley</td>
<td>304</td>
<td>9781119085294</td>
</tr>
</tbody>
</table>
Overview:

The Top Nine Factors of Data Protection Control Effectiveness and Sustainability
## Terminology

### Cybersecurity
- Protection of digital data and information systems against electronic attacks. The measures taken to protect information systems that store, process or transmit electronic data against the unauthorized access, use, disclosure or harm. Cybersecurity is limited to the protection of electronic/digital data and information only, and exclude protection of physical data.

### Information Security
- The ongoing process of exercising due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, disruption or distribution. It includes the design, implementation and evaluation of countermeasures that provide confidentiality, integrity, and availability to counter, prevent, detect, and document threats to digital and non-digital information assets.

### Information Assurance
- The overarching approach for identifying, understanding, evaluating and managing risks through an organization’s use of information and information systems. It is concerned with the lifecycle of information through the objectives of maintaining the following attributes: confidentiality, integrity, availability, non-repudiation, authentication, possession and utility.

  Information Assurance is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.

### Privacy
- The ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. It is the requirement to maintain control over one’s personal information to determine when, how, and to what extent information is communicated to others. Privacy concerns exist wherever uniquely identifiable data relating to a person are collected and stored, in digital form or otherwise, how data are collected, stored, and associated, and who is given access to information. Other issues include whether an individual has any ownership rights to data about them, and/or the right to view, verify, and challenge that information.
Terminology

Data Protection
- The act of protecting the possession, confidentiality and integrity and authorization of personal and corporate data where controls are implemented to ensure consent and choice, collection limitation, data minimization, use, retention, limitation of disclosure, accuracy and quality, openness, transparency and notice, individual participation and access, accountability, purpose legitimacy, and information security. Data protection focuses on the protection of sensitive personal and corporate data that is collected, accessed, updated, stored and disposed of by people and information systems. It includes, inter alia, names, contact information such as physical addresses, phone numbers and email addresses, medical history, banking details, credit ratings, employment records, religious and political opinions.

- Therefore, data protection goes well beyond information security. It is a more comprehensive term which is inclusive of all data elements and selective security measures. It is usually covered by various data protection laws applicable to a specific region, such as the European Union’s General Data Protection Regulation (GDPR). Data protection, although mostly focusing on personal data, can also be extended to include the protection of about sensitive corporate data which, when compromised, can harm a corporate entity.

Security Event
- Anything that happens that could potentially have information assurance implications. A security event can be any event such as access, use, disclosure, disruption, modification, or destruction of data, information or information systems and other actions that can impact information assurance with the potential to compromise the confidentiality, possession, control, integrity, authenticity, availability, and utility of information systems or data.
For example, a security event can be a system crash, packet floods, unauthorized use of system privileges, etc.
Terminology

Security Incident
• Any observable occurrence in a system or network that violates an organization’s security or privacy policies, or compromises the integrity, confidentiality, availability, possession or utility of an information asset. For example, a suspected, attempted, or imminent threat of unauthorized access, use, disclosure, modification, or destruction of data or a system component.

Security Breach
• An act from outside an organization that bypasses or contravenes security policies, practices, or procedures. A similar internal act is called security violation. A security breach can be any confirmed security incident that involves access, use, disclosure, disruption, modification, or destruction of restricted information systems. A security breach differs from a data breach.

Data Breach
• When the security or privacy of data that should be protected is compromised due to the unauthorized acquisition, access, use, or disclosure, or the accidental or unlawful destruction, loss or alteration of protected data. It includes all security incidents where sensitive, protected or confidential data were confirmed to be copied, transmitted, viewed, stolen, used, or altered by a system or individual not unauthorized to do so. A data breach is an incident that results in the confirmed compromise—not just potential exposure—of data to an unauthorized party, as a result of accidental or unlawful breaches of security. It is a violation, transgression, infringement, a gap or breakthrough of restrictions and trust placed on the data and/or the information systems that store, process or transmits the data.

Data Compromise
• See Data Breach - The terms data compromise and data breach can be used interchangeably. Data compromise refers to the exposure of data to elements that violates the restriction placed on data to ensure the trust in its confidentiality, availability, integrity, use, possession, control, authenticity and utility.
Terminology

Sustainability

- A security control, and a control environment can be considered “sustainable” when an organization demonstrates the capacity, capability, competence and commitment needed to maintain the required level of configuration, functionality and performance of security controls to meet control design specifications and data protection objectives over extended periods of time.

  The level of sustainability can be measured by monitoring the amount of deviations from the established standard of control operation and performance, and tracking the amount of effort, resources (cost, people and time) required to maintain the required status (i.e. performance and effectiveness) of data protection operations.

- See Control Robustness and Control Resilience.

Technical sustainability:
the investment needed to maintain required configuration and functionality of system components.

Administrative sustainability:
the investment needed to communicate and maintain required documentation, and procedures.

Operations sustainability:
the investment needed to maintain required to monitor the operation and performance of a control, to ensure required level of effectiveness.
What prevents data compromises: sustainability (sustainable effectiveness)

The sustainability of a control environment can be measured by the level of robustness and resilience built into control systems and the control environment. Robustness and resilience of the control environment is achieved by maintaining the required capacity, capability, competence and commitment to effectively support the development of a mature data protection program.

QUOTE: 2018PSR - “Sustainable controls are extremely relevant to payment security. They can only be achieved in an environment that is measured and monitored for performance and that identifies weaknesses as they develop. To function well, payment systems need to be regularly maintained with reliable and measurable performance standards.”

“Lack of sustainable control environments remains a top contributor and precursor to ineffective controls, which in turn become susceptible to data breaches.”

Organizations achieve sustainability by design; i.e., by building sustainability into the functional, operational specifications of the compliance program and reinforcing it through frequent education, training and awareness campaigns.”
The 9 Factors of Control Effectiveness and Sustainability

- Control Environment
- Control Design
- Control Risk
- Control Robustness
- Control Resilience
- Lifecycle Management
- Performance Measurement
- Maturity Measurement
- Self-Assessment
The 9 Factors

Factor 1: Control Environment  The sustainability and effectiveness of controls depend on a healthy control environment.

Factor 2: Control Design  Proper control operation to meet security control objectives depends on sound Control Design.

Factor 3: Control Risk  Without on-going maintenance (security testing, risk management, etc.), controls can degrade over time and eventually break down. Mitigation of control failures requires integrated management of Control Risk.

Factor 4: Control Robustness  Controls operate in dynamic business and ever-changing threat environments. They must be robust to resist unwanted change to remain functional and perform to specifications (config standards, access control, system hardening, reviews etc.).

Factor 5: Control Resilience  Security controls can potentially still fail, despite adding layers of control for increased robustness, therefore control resilience with proactive discovery and quick recovery from failure is essential for effectiveness and sustainability.

Factor 6: SCLM  Security Control Lifecycle Management - to achieve all of the above, monitor and manage security controls throughout each stage from inception to retirement.

Factor 7: Performance Management  Establishing performance standards (define, communicate, measure)

Factor 8: Maturity Measurement  Prevent a stagnant control environment through continuous improvement

Factor 9: Self-Assessment  Achieving all of the above requires in-house proficiency; capacity, capability, competency and commitment.
The Top Nine Factors:  Control Effectiveness and Sustainability

1. Design and maintain a control environment
2. Design and integrate security controls
3. Measure the control risk of each control (inherent risk x residual risk x detection risk)
4. Enhance control robustness
5. Enhance control resilience
6. Maintain control lifecycle management
7. Performance Management
   - Integrated monitoring and reporting
8. Maturity Measurement
   - Continuous improvement
9. Control Evaluation Self-Assessment
F1: Control Environment

An effective control environment is:

“an environment in which competent people understand their responsibilities, the limits of their authority, and are knowledgeable, mindful and committed to doing what is right and doing it the right way.”

F2: Control Design

Documented control profiles:

1. **Control Objective**: define objective of the control / control system
2. **Owner**: assigned ownership and responsibilities
3. **Function**: management, procedural, technical etc.
4. **Control type**: preventative, detective, corrective, directive
5. **Architecture**: system-specific, common, hybrid
6. **Control Risk**: control to risk matrix / mapping
7. **Control Testing**: test procedures and standards
8. **Implementation**: specifications, scope, dependencies
9. **Operation**: specifications, scope, processes, dependencies
10. **Maintenance**: specifications, scope, processes
11. **Performance Metrics**: KPI’s and metrics to measure performance
12. **Governance**: related policies, standards and frameworks
The Control Landscape

Control Architecture Allocations:

- **System-Specific Controls**
  Controls that provide a security capability for a particular information system only

- **Common Controls**
  Controls that provide a security capability for multiple information systems

- **Hybrid controls**
  Controls that have both system-specific and common characteristics
Detecting Low Proficiency

Ask the right questions:

• Which controls are effective? (and not merely “in place”)
• Which controls fail? When and how?
• What is the impact when a control fails?
• How soon do you detect control failure?
• How quickly do you restore failed controls?
• Was the root cause of failure remedied?

Top performers proactively track the failure rate of their security controls.

Mediocre performers follow a “break / fix" model year-after-year.

Low performers wait for an assessor to point out the control failures.
Control Deficiencies

**Deficiency in design exists when:**

a. a control necessary to meet the control objective is missing, or

b. an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met.

**Deficiency in operation exists when**

a. a properly designed control does not operate as designed, or

b. when a person performing the control does not possess the necessary competence or authority to perform the control effectively.

Source: PCAOB Public Accounting Oversight Board Auditing Standard No. 5 available online at https://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5_Appendix_A.aspx
F3: Control Risk

The likelihood and impact of control failure, due to absence or failure of control design or operation.

• Typically caused by controls losing effectiveness over time.
• Continuously measure and monitor:
  • \( \text{Inherent risk} \times \text{Residual risk} \times \text{Detection risk} \)

“Controls are effective only as long as they mitigate risk to an acceptable risk tolerance. They are often sustainable merely by luck—certainly not by design.”

~ Verizon 2017 Payment Security Report
### F4: Control Robustness

**Robustness:** "the ability of a system to resist change without adapting its initial stable configuration"

The ability of a control, and/or the control environment, to absorb disturbance and still retain its basic structure and viability to meet control objectives, without the need for intervention.

<table>
<thead>
<tr>
<th>Control Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Design</td>
</tr>
<tr>
<td>Control Risk</td>
</tr>
<tr>
<td><strong>Control Robustness</strong></td>
</tr>
<tr>
<td>Control Resilience</td>
</tr>
<tr>
<td>Lifecycle Management</td>
</tr>
<tr>
<td>Performance Measurement</td>
</tr>
<tr>
<td>Maturity Measurement</td>
</tr>
<tr>
<td>Self-Assessment</td>
</tr>
</tbody>
</table>
Capacity, Capability, Competence, Commitment

• **Capacity**  
  Required number of resources; people, process and technology. You cannot measure, manage, and improve that which you do not have.

• **Capability**  
  Ability to direct and apply resources to perform data protection tasks and the processes to support them.

• **Competence**  
  Having the skills, knowledge and experience to establish and maintain an operational control environment. This requires a level of maturity in business process management to achieve quality (repeatability and consistency) in each step of the control lifecycle.

• **Commitment**  
  Assurance that management and employees will consistently adhere to data protection and compliance programs.

Data protection with consistency: doing the right things, in the right manner and at the right time.
Control Robustness and Resilience

Introduction of the “4 C’s Model”:

Control robustness relates to the ability of a control to remain effective in meeting its control objective, despite environmental disruption.

A robust control environment is more resistant to attacks and can operate effectively over extended periods of time.

Resilience, in its simplest form, is often defined as the ability to bounce back (or forward). Controls that are able to rapidly recover from disruptive events to resume operating effectively after being exposed to adverse events.

<table>
<thead>
<tr>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>An organization’s “data protection capacity” can be described as the required amount of resources available to produce or deliver a determined amount of data protection objectives over an extended period. Data protection program performance depends heavily on the organization’s ability to acquire and maintain the required number of resources, i.e., the people, processes, technology, time and attention needed to support the program. A threshold of resources is required for a successful program. You cannot measure, manage and improve what your teams cannot capture.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ability of the organization to direct and apply resources to perform data protection tasks and the processes to support them. Individuals and teams must have the skills and capacity to perform the necessary actions. You need to determine whether the system components (people, processes, and technology) within your control environment have the awareness, knowledge and understanding to achieve the required standard of performance. Capability does not, however, mean there is an actual desire to apply those skills. They may just have the capability, but motivation and incentives are needed to make data protection and compliance a priority.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Competence</th>
</tr>
</thead>
<tbody>
<tr>
<td>You need to have the knowledge, skills and experience to establish and maintain a sustainable operational control environment. It requires a level of maturity in business process management to achieve quality (repeatability and consistency) in each step of the control life cycle. Agility and flexibility also are needed to change and develop, in light of new situations, and to deal with constant changes in the threat and regulatory landscapes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Commitment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assurance that management and employees will consistently adhere to data protection and compliance programs is critical. It demands consistency of application and across-the-board discipline to adhere to standards and programs. In other words, consistency in doing the right things, in the right manner and at the right time.</td>
</tr>
</tbody>
</table>
F5: Control Resilience

Goals.

• **Anticipate**: Maintain a state of informed preparedness.
• **Withstand**: Continue essential functions despite attacks.
• **Recover**: Restore functions to fullest extent possible.
• **Evolve**: Change functions to minimize future adverse effects.

*Source: MITRE, “Cyber Resiliency Basics” by Rosalie McQuaid, November 15, 2013*

https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/cyber-resiliency-basics
Lines of Defense

For data protection to be effective, robust and resilient most organizations deploy four lines of defense:

1. The individual at the front line that operates a system or handles certain data
2. The risk management or compliance team responsible to guidance and enforce risk and compliance responsibilities
3. Internal audit to monitor adherence to policies and standards, and to cross check the performance of the risk and compliance teams
4. External auditor and regulatory bodies monitoring compliance to standards and agreements.

You need to manage maintain the “4C’s” (Capacity, Capability, Competence, Commitment) in each of the four lines of defense.
Security Control Lifecycle Management

Introduced in the 2016 & 2017 Payment Security Reports

Security control lifecycle management (SCLM) defines the control support requirements over the life of the control or control system—the journey from its conception and design to the retirement of a control. It’s essential that organizations understand how each stage of the control lifecycle influences underlying support processes, operational efficiency and effectiveness of security controls.

The integration of SCLM into security compliance programs helps to prevent the continued degradation of the control environment and can enable and support early identification of control weaknesses.
F7: Performance Measurement

1. Establish **performance standards** for each component of the control environment.

2. Maintain performance measurement program on:
   a. Control environment
   b. Control design, risk, robustness, resilience
   c. Control lifecycle management
   d. Defined metrics

3. Provide ongoing feedback, guidance on corrective actions.
F8: Maturity Measurement

**Security Control Performance & Maturity**

1. **Measuring Control Design:**
   How well it should work in theory

2. **Measuring Control Implementation:**
   How well it actually performs in practice

3. **Measuring Control Monitoring:**
   How we know that it’s still working

4. **Measuring Control Evaluation:**
   How frequently we evaluate effectiveness & efficiency

5. **Scoring Control Effectiveness**:
Maturity Measurement

In the face of continuing high-profile data breaches, organizations are under pressure to demonstrate control effectiveness and higher degrees of data protection performance—underscoring the need for true data protection proficiency. Maturity models provide a roadmap toward higher proficiency.

Measuring the performance of a control environment and applying metrics for informed, data-driven decision making creates the foundation for structured growth of data protection and compliance capabilities.

Based on our field observations, less than a quarter of organizations apply security metrics, such as control coverage, control effectiveness and operational performance metrics.

![Maturity Measurement Diagram]

Figure 10. Use of process maturity models
Control Effectiveness: Observations and Analogies

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.
Control Effectiveness: Observations and Analogies
QSA Horror Story
Terrifyingly short

**Question:** How long would you make your password if storing primary account numbers (PANs) in clear text?

During one assessment, a QSA found an admin account with access to 70 million PANs protected by the weakest password we’ve ever seen - a **single character**!

The operator’s defense was that it was a “special character”.

#lame_excuse
Control Effectiveness: Maturity

<table>
<thead>
<tr>
<th>Control effectiveness</th>
<th>Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully effective</td>
<td>Nothing more to be done except review and monitor the existing controls.</td>
</tr>
<tr>
<td>Substantially effective</td>
<td>Most controls are designed correctly but more work to be done on design, validation.</td>
</tr>
<tr>
<td>Partially effective</td>
<td>Some controls are designed correctly and operate effectively, but many need work to ensure they address root causes and/or contributing factors.</td>
</tr>
<tr>
<td>Largely ineffective</td>
<td>Significant control gaps exist, or controls do not operate effectively at all.</td>
</tr>
<tr>
<td>None or totally ineffective</td>
<td>Management has no confidence that any degree of control is being achieved.</td>
</tr>
</tbody>
</table>
Control Effectiveness

Practical example of application:

- Measuring Control Effectiveness
- Measuring Control Maturity

Example of how to measure control effectiveness

An example of applying the DIME model—“Design, Implementation, Monitoring, Evaluation” for scoring the effectiveness of security controls in four steps:

1. Measuring control design: How well it should work in theory
2. Measuring control implementation: How well it actually performs in practice
3. Measuring control monitoring: How well it is still working
4. Measuring control evaluation: How frequently we evaluate effectiveness and efficiency

NOTE: If either design or implementation is zero, then total score becomes zero.

Source: Dr John Mitchell, LHS Business Controls

Scoring:

1. Measuring control design
   - How well the control should work, in theory, if it’s always applied as intended.
   - Designed to reduce risk effective
     - Designed to reduce risk partially effective
     - Designed to reduce risk ineffective
   - 0 1 2 3

2. Measuring control implementation
   - Control is not applied or applied incorrectly
     - Control is sometimes incorrect or applied
     - Control is always applied as intended
   - 0 1 2 3

3. Measuring control monitoring
   - Control is not monitored or monitored infrequently
     - Control is monitored frequently
     - Control is always monitored for effectiveness/efficiency
   - 0 1 2 3

4. Measuring control evaluation
   - Control is never evaluated or evaluated very infrequently
     - Control is occasionally evaluated for effectiveness/efficiency
     - Control is regularly evaluated for effectiveness/efficiency
   - 0 1 2 3

5. Scoring control effectiveness (no weighting)
   - Apply DIME:
     - 2 out of 3
     - 2 out of 3
     - 2 out of 3
     - 1 out of 3
   - Total = 6/12 = 50% total effectiveness

Figure 21. The DIME model
Measuring Control Effectiveness

How To - Example:

5. Scoring Control Effectiveness (No Weighting)

Apply DIME:

<table>
<thead>
<tr>
<th>Control</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td>2 (3)</td>
</tr>
<tr>
<td>Implementation</td>
<td>3 (3)</td>
</tr>
<tr>
<td>Monitoring</td>
<td>2 (3)</td>
</tr>
<tr>
<td>Evaluation</td>
<td>1 (3)</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>8 (12)</td>
</tr>
</tbody>
</table>

**NOTE:** If either Design, or Implementation is zero then total score becomes zero

Source: John Mitchell - Measuring Control Effectiveness
GRC 2.0 - Breaking Down The Silos, ISACA Ireland Conference – 3rd October 2014
Self-Assessment

Self-assessment is an in-house organizational competency to establish, evaluate and record measurable outcomes for each of the 9 Factors that respectively also includes the assessment of self-assessment capability.

The “four Cs” as framework to develop a self-assessment program:

- evaluate the required number of resources (capacity),
- the ability to direct and apply resources (capability),
- the skills, knowledge and experience (competence),
- and the assurance from management to consistently adhere to compliance and data protection requirements (commitment).

The shortage of skilled professionals is not a new problem.

- In 2017, the US employed nearly 780,000 people in cybersecurity positions, with approximately 950,000 current cybersecurity openings and the same number of openings in Europe.
- Several years ago, estimates were that by 2014, the information security industry would experience a shortage of more than a million security professionals across the globe.
- In 2015, Symantec expected the demand for cybersecurity talent to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million.
- A year later, a skills gap analysis from ISACA estimated a global shortage of 2 million cybersecurity professionals by 2019.
- It is now predicted that 9.5 million cybersecurity job openings will exist by 2021.

When struggling with empty positions or a lack of qualified individuals, businesses should find every opportunity to support their currently employed skilled professionals to maximize the value they can deliver. Organizations that rely on external parties to evaluate their internal control environments need to fully integrate learning opportunities to develop their own capabilities for evaluating control effectiveness, control risk, and measuring capability maturity to continue a path toward self-reliance.
F9: Control Self-Assessment

- Establish self-assessment program.
- Standardize assessment methods.
- Develop and maintain assessment procedures.
- Build internal assessment competency to measure, monitor and proactively manage factors.
- Self-assess your Capacity, Capability, Competence, and Commitment.
# Integrated Implementation Model

Measuring sustainability and effectiveness by evaluating your 4C’s for each factor across every Line of Defense (SE = 4C x 9F x LoD)

<table>
<thead>
<tr>
<th>FACTORS</th>
<th>Capacity</th>
<th>Capability</th>
<th>Competence</th>
<th>Commitment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluate your 4C’s across all 9 Factors for each Line of Defense:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Individual Accountability</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2. Risk Management &amp; Compliance Team</td>
<td>✔</td>
<td>✔</td>
<td>?</td>
<td>✔</td>
</tr>
<tr>
<td>3. Internal Audit</td>
<td>✔</td>
<td>?</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>4. External Audit, Regulators</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>?</td>
</tr>
<tr>
<td>5. Control Environment</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>6. Control Design</td>
<td>✔</td>
<td>✔</td>
<td>?</td>
<td>✔</td>
</tr>
<tr>
<td>7. Control Risk</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>8. Control Robustness</td>
<td>✔</td>
<td>?</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>9. Control Resilience</td>
<td>✔</td>
<td>?</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>10. Lifecycle Management</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>?</td>
</tr>
<tr>
<td>11. Performance Management</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>?</td>
</tr>
<tr>
<td>12. Maturity Measurement</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>?</td>
</tr>
<tr>
<td>13. Self-Assessment</td>
<td>?</td>
<td>✔</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>
Apply What You Have Learned Today

Lessons learned:

• **Measure twice, cut once.**
  You seldom get a 2nd change at preventing data breaches.

• **Develop your in-house proficiency.**
  Confidence and predictable outcomes are achieved through knowledge, skill, and experience.

• Do not place mission critical tasks in the hands of unqualified resources.
Breach of PCI-DSS compliant company?

Data for the data breach correlation section is separate from our PCI DSS assessment dataset. It comes from investigations on organizations following a breach of payment card data.

These investigations, 237 across 35 countries, were carried out by our PFI group between 2010 and 2017. It is also part of the Verizon Data Breach Investigations Report.

In the last 12 years, not a single organization that we have assessed following a data breach was fully PCI DSS compliant at the time of the breach.

Overall, breached organizations have significantly lower compliance — there’s a 42pp difference in total average PCI DSS Compliance.
Value of PCI Security Compliance

The following is a list of five payment card data breach scenarios that can apply to organizations that are mandated to comply with the PCI Security regulation. Each scenario indicates the state of PCI Security compliance at the time of the data compromise. They are listed in order of data protection maturity.

1. The organization did not initiate a PCI Security compliance program. They have not yet introduced controls that are aligned to PCI Security requirements into their control environment, and have not attempted to validate their compliance. They are deemed non-compliant with PCI DSS at the time of the compromise.

2. The organization initiated a PCI Security compliance program, but have not completed the implementation of the required security controls, and have not validated their compliance. They are deemed non-compliant with PCI DSS at the time of the compromise.

3. The organization completed the implementation of their required PCI Security controls and validated their compliance, but subsequently did not maintain their security controls. They are deemed non-compliant with PCI DSS at the time of the compromise.

4. The organization implemented all required PCI Security controls, validated their compliance, and maintained all their controls. They subsequently experienced a data compromise while in full compliance with the standard. They will be deemed to be compliant with PCI DSS at the time of the compromise. This means that the attackers circumvented multiple layers of controls and that the standard is therefore demonstrably flawed as a baseline level of protection.

5. The organization is validated to be in full compliance with PCI Security requirements, and they maintain their compliance year round. In addition they also implement and maintain various other security frameworks and standards that go above and beyond PCI Security requirements. They will be deemed to be compliant with PCI DSS at the time of a compromise.

There are no publicly known cases of scenarios 4 and 5 ever occurring.

Sidenote: The PCI Security standards are not infallible and does not offer any guarantee of effectiveness to prevent data compromises. Various aspects of the PCI Data Security standard need to be improved. Yet, no disclosed case exist of any organization every experiencing a confirmed payment card data compromise while they were full compliance with any of the PCI Data Security standards, since the release of version 1.1. Such a case has to date not yet been made known.
What prevents data compromises

When people are asked what prevents sensitive data from being compromised by hackers, most people, including IT and Information Security professionals will include various security technologies on top of their list of countermeasures – such as “firewalls”, “anti-virus”, and “password access control systems”. Some will include “system hardening, strong authentication, encryption, and tokenization” on their list of endpoint-based technology defenses.

However, few will include “integrated risk-based decision making”, “security and risk-based processes”, “change control”, and “maintaining a sustainable control environment” – which are the more likely contributors of effective data protection.

The top 3 key factors that prevent data compromises:

1. Integrated risk-based decision making, baked into the operational culture of the organization
2. The process and capability maturity to design and maintain the effectiveness of the control systems
3. The process and capability maturity to design and maintain the sustainability of the control environment