# Achieving Excellence, Success & Value Through Best Practices in Cybersecurity Leadership & Management

William Favre Slater, III
Chicago, Illinois
May 21, 2020

# Agenda

- Principles
- Why?
- Example Audit Information
- Compliance Frameworks
- Understanding Security Costs vs. Asset Value & the Natures of Risks
- Understanding Return on Security Investment (RoSI)
- Costs of Compliance Vs. Non-Compliance
- The Answer: Better Cybersecurity Leadership & Management
- Select the Cybersecurity Management Framework For Organization
- Build a Cybersecurity Capability Maturity Roadmap
- Baseline Your Cybersecurity Management Program
- Using Effective Cybersecurity Metrics AND Continually Monitor & Measure Your Cybersecurity Program
- Hold All Team Members Accountable to Continually Perform Adapt & Improve
- Understand and Communicate the Current & Future Costs & Value to Your Sponsors
- Regularly Report the Results to Management
- Continually Grow and Get Smarter
- Conclusion

# Principles

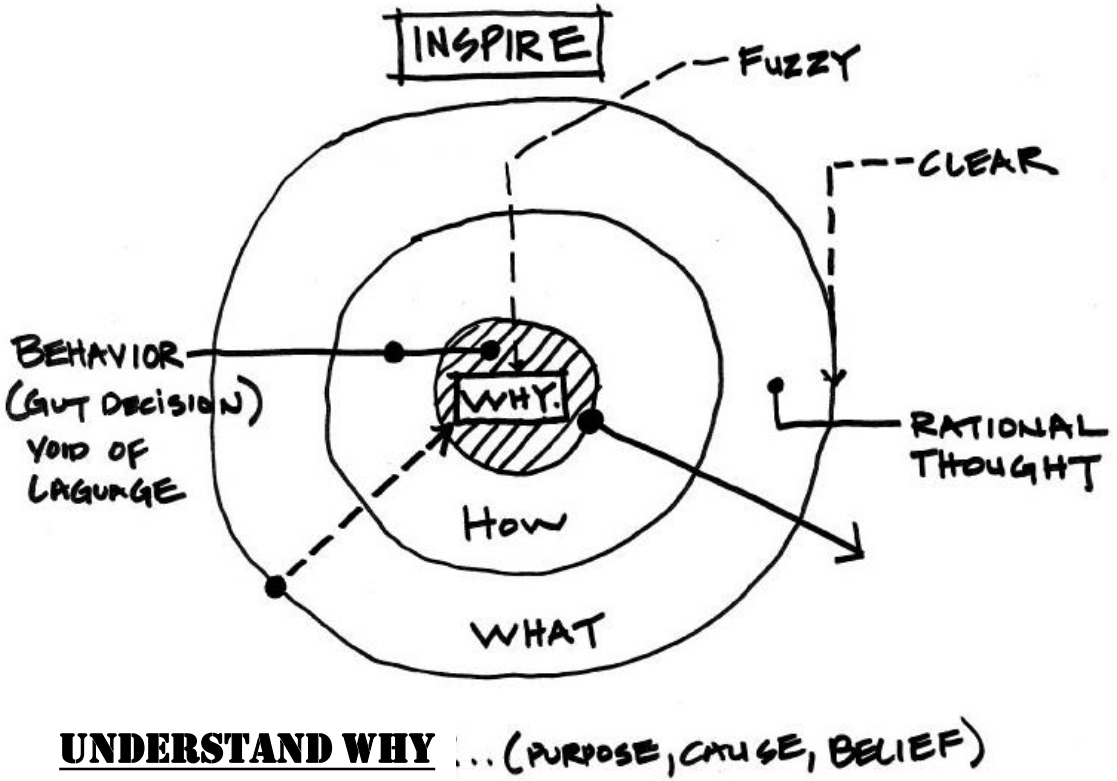
Cybersecurity and the Prudent Management of Cybersecurity Resources are two of the hottest and most important topics for organizations in the 21st Century.

In the 21st century Cybersecurity has become the set of practices that cover the management of information technology security including access control systems and methodology, business continuity and disaster recovery planning, legal issues in information system security, ethics, computer operations security, physical security and security architecture & models using current standards and models.

Cybersecurity has matured into a discipline that includes its own terms, frameworks, standards, and best practices.

If these frameworks, standards, and best practices are understood and properly applied in a mature and prudent way, they offer the best hope of coherently managing business environment CyberRisks in a world of constantly evolving complex and persistent CyberThreats.

# *Why?*




**UNDERSTAND WHY** ...(PURPOSE, CAUSE, BELIEF)

For more information about Start with WHY, please view Simon Sinek's legendary presentation: https://www.youtube.com/watch?v=qp0HIF3SfI4

# *Example 01 from an ISO 27002 Audit*

**Requirements to establish and maintain Information Security Management System (ISMS).**

1. **Organizational context and stakeholders**
2. **Information security leadership and high-level support for policy**
3. **Planning an information security management system; risk assessment; risk treatment**
4. **Supporting an information security management system**
5. **Making an information security management system operational**
6. **Reviewing the ISMS performance**
7. **ISMS Improvement**

# *Example 02 from an ISO 27002 Audit*

| ISO27001 Requirement | Formal Implementation | Partial Implementation | Tribal Knowledge | Non-existent |
|---|---|---|---|---|
| Organizational context and stakeholders | | ✔ | | |
| Information security leadership and high-level support for policy | | ✔ | ✔ | |
| Planning an information security management system; risk assessment; risk treatment | | ✔ | ✔ | ✔ |
| Supporting an information security management system | | | | ✔ |
| Making an information security management system operational | | | | ✔ |
| Reviewing the ISMS performance | | | | ✔ |
| ISMS Improvement | | | | ✔ |

# Example 03 from an ISO 27002 Audit

- Provides a list of commonly accepted control objectives and best practice controls to be used as implementation guidance when selecting and implementing controls for achieving information security.

- This standard contains 14 security control clauses collectively containing a total of 35 main security categories and 115 controls.

# Example 04 from an ISO 27002 Audit

| ISO27002 Domains | Objective | # of Controls | Formal Controls | Tribal Knowledge | Non-existent | N/A |
|---|---|---|---|---|---|---|
| Information Security Policies | policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties | 2 | | 2 | | |
| Organization of Information Security | information security responsibilities should be defined and allocated | 7 | | 7 | | |
| Human Resource Security | ensure employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. | 6 | 2 | 4 | | |
| Asset Management | identify organizational assets and define appropriate protection responsibilities | 10 | 2 | 8 | | |
| Access Control | limit access to information and information processing facilities | 14 | | 14 | | |
| Cryptography | ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. | 2 | 2 | | | |
| Physical and environmental security | prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. | 15 | 6 | 9 | | |
| Operations Security | ensure correct and secure operations of information processing facilities | 14 | 1 | 12 | 1 | 0 |

# Example 05 from an ISO 27002 Audit

| ISO27002 Domains | Objective | # of Controls | Formal Controls | Tribal Knowledge | Non-existent | N/A |
|---|---|---|---|---|---|---|
| Communications Security | networks should be managed and controlled to protect information in systems and applications | 7 | 1 | 6 | | |
| Systems Acquisition Development and Maintenance | information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems | 13 | | 14 | | |
| Supplier Relationship | identify organizational assets and define appropriate protection responsibilities | 5 | | 4 | | |
| Information Security Incident Management | ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses | 7 | | 7 | | |
| Information Security Aspects of Business Continuity Management | determine requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster | 4 | | 4 | | |
| Compliance | avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. | 8 | | 4 | 4 | |
| **Totals** | | **114** | **14 (12%)** | **95 (83%)** | **5 (4%)** | **0** |

# Example 06 from an ISO 27002 Audit

| ISO27002 Policies and Procedures | GoHealth Policy? | Develop or Enhance Policy? | Develop Procedure? | Comments |
|---|---|---|---|---|
| Access Control | | ✓ | ✓ | |
| Information Classification and Handling | ✓ | ✓ | ✓ | |
| Physical and Environmental Security | ✓ | ✓ | ✓ | |
| Acceptable Use of Assets | ✓ | ✓ | | |
| Clear Desk and Clear Screen | | ✓ | | |
| Mobile Devices and Teleworking | ✓ | ✓ | | *In Acceptable Use Policy* |
| Restrictions on Software Installations and Use | ✓ | ✓ | | *In Acceptable Use Policy* |
| Backup and Recovery | | ✓ | ✓ | |
| Information Transfer | ✓ | ✓ | | *In Encryption Policy* |
| Protection from Malware | ✓ | ✓ | | *In Firewall Mgmt. Policy* |
| Management of Technical Vulnerabilities | ✓ | ✓ | | *In Risk Mgmt. Policy* |
| Cryptographic Controls | ✓ | ✓ | ✓ | |
| Communications Security | ✓ | ✓ | ✓ | *In Firewall Mgmt. Policy* |
| Privacy and Protection of Personally Identifiable Information | | ✓ | ✓ | |
| Supplier Relationships | | ✓ | ✓ | |
| Risk Assessment | ✓ | ✓ | ✓ | |
| Governance and Planning | ✓ | ✓ | | *In Information Security Policy* |
| Security Awareness Program | ✓ | ✓ | ✓ | |
| Totals | 13 | 7/11 (18) | 10 | |

# Example 07 from an ISO 27002 Audit

| Information Security Management and Organization | | | |
|---|---|---|---|
| **Summary Gaps/Weaknesses** | **Recommendation** | **Deliverables** | **Effort** |
| • Incomplete Info Sec Governance and Planning Policy<br>• No specific ISO function and role<br>• Informal Info Sec planning in management meetings<br>• Roles and responsibilities are often "blurred"<br>• Limited segregation of duties | • Define and assign ISO role<br>• Create Information Security function<br>• Develop Security Management Framework<br>• Define roles and responsibilities<br>• Define segregation of duties/responsibilities<br>• Formalize Info Sec as part of Sr. Mgmt meetings | • Management planning template<br>• Info Sec roles and responsibilities<br>• Info Sec Governance and Planning Policy<br>• SOD matrix | 1 week |

| Information Security P&P Development | | | |
|---|---|---|---|
| **Summary Gaps/Weaknesses** | **Recommendation** | **Deliverables** | **Effort** |
| • No central ownership and assigned SMEs to maintain P&Ps going forward<br>• Lack of additional 7 Policies<br>• Existing 11 policies missing ISO27002 requirements<br>• No procedures to support 10 policies<br>• No process to periodically update P&P | • Assign ownership and SMEs for all P&P<br>• Develop 7 new policies<br>• Enhance existing 11 policies to ISO standard<br>• Develop 10 procedures<br>• Socialize and adopt P&Ps | • Set of ISO 27001 policies and procedures<br>• Finalize scope of ISMS<br>• Socialization and adoption (optionally handled by GoHeath) | 4 weeks |

# Example 08 from an ISO 27002 Audit

| Risk Assessment | | | |
|---|---|---|---|
| **Summary Gaps/Weaknesses** | **Recommendation** | **Deliverables** | **Effort** |
| • No formal owner of Risk Assessment<br>• Policy defined but needs enhancement<br>• No procedure to risk rank threats and vulnerabilities<br>• No Risk Registers and Risk Treatment Plan | • Assign ownership of risk assessment and roles and responsibilities<br>• Enhance risk management policy based on ISO 27001/27002<br>• Develop risk assessment rating approach<br>• Develop risk registers and risk treatment plan<br>• Conduct Risk Assessment based on procedure | • Enhanced Risk Management Policy<br>• Risk assessment procedure<br>• Risk assessment work sheets<br>• Risk Register<br>• Risk Treatment Plan | 3 weeks |

| Information Classification | | | |
|---|---|---|---|
| **Summary Gaps/Weaknesses** | **Recommendation** | **Deliverables** | **Effort** |
| • No formal owner of Information Classification<br>• Policy defined but needs enhancement<br>• No procedure to classify the confidentiality, integrity and availability of information<br>• No assigned owners of information | • Enhance Information Classification policy to include ISO27002 guidelines<br>• Develop procedure to conduct information classification<br>• Develop information classification worksheets containing ratings, ownership, handling and level of protection<br>• Conduct Information Classification based on procedure | • Enhanced Information Classification Policy<br>• Information Classification procedure<br>• Information Classification work sheets to be stored in GoHealth repository | 2 weeks |

# Example 02 from an ISO 27002 Audit

| Controls Development/Enhancement | | | |
|---|---|---|---|
| **Summary Gaps/Weaknesses** | **Recommendation** | **Deliverables** | **Effort** |
| • 83% of controls need to be formalized<br>• Develop 4% of non-existent controls<br>• Control activities are not designed with who performs the control, frequency and type of evidence | • Design control according to GoHealth environment with control owner, frequency and type of evidence<br>• Socialize and adopt control<br>• Match control to risks to finalize risk registers and risk treatment plan | • Set of ISO 27002 controls for 14 domains<br>• Completed Risk Registers<br>• Completed Risk Treatment Plan<br>• Socialization and Adoption (optionally handled by GoHealth) | 4 weeks |

| ISMS and Controls Monitoring | | | |
|---|---|---|---|
| **Summary Gaps/Weaknesses** | **Recommendation** | **Deliverables** | **Effort** |
| • No current compliance process to periodically monitor adoption and execution of controls<br>• No process to fine-tune process/controls when exceptions are observed or new process/technology is implemented | • Process for periodic assessment will be included in the compliance policy<br>• Develop procedure to conduct periodic controls assessment, reporting, escalation and resolution tracking in compliance policy<br>• Prepare entire ISMS and internal controls assessment for ISO certification | • Report of ISMS and controls assessment<br>• Package ISMS and internal controls assessment in preparation for ISO certification<br>• Assist in the selection of ISO 27001 certified auditor(s)<br>• Assist in the ISO certification process | 1 week |
| | | Total weeks | 14 |

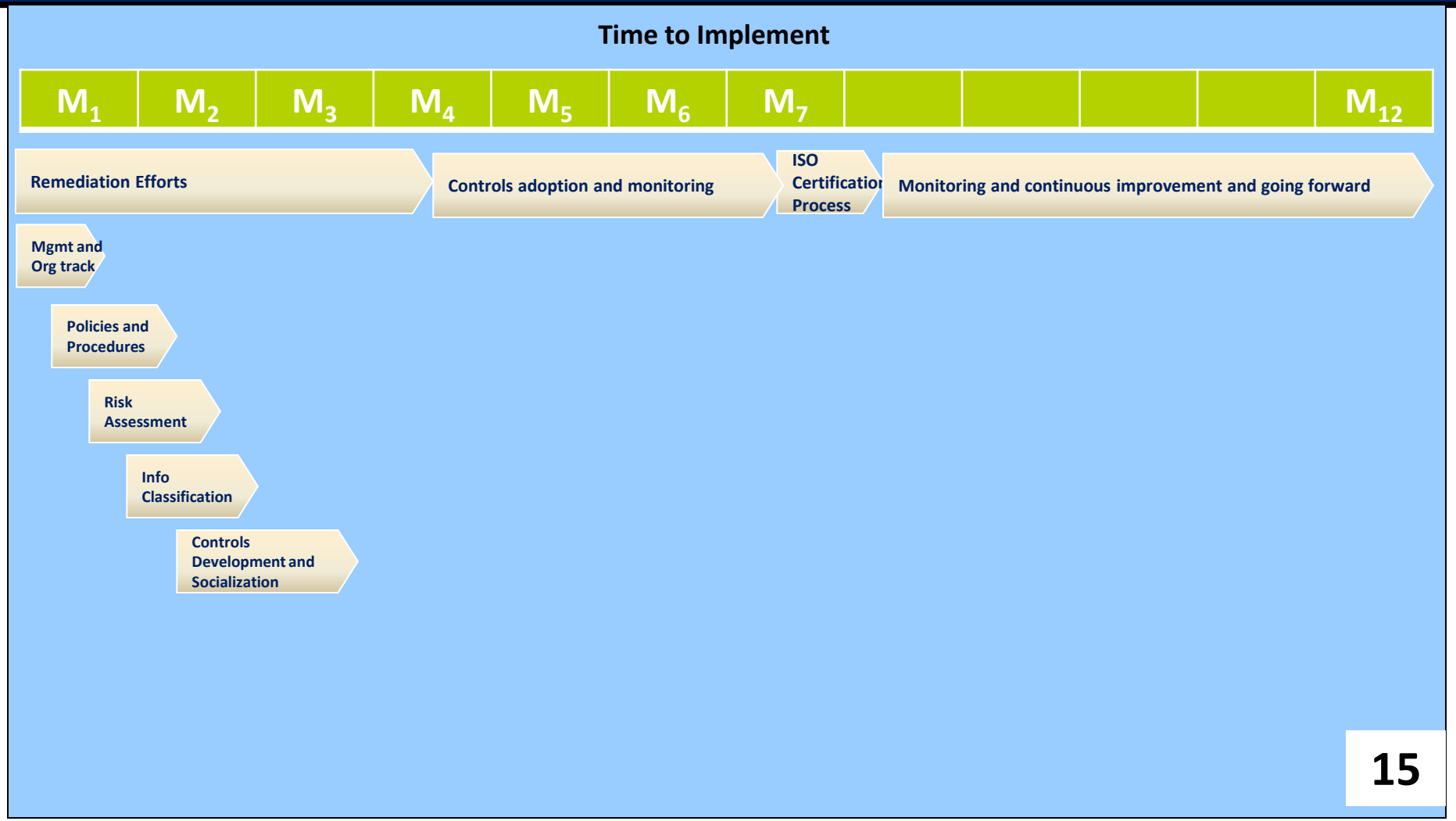
13

# *Example 09 from an ISO 27002 Audit*

## Detailed Report – (Excerpt)

| Requirement/Control Statement | Observations | Priority | Recommendation | Effort |
|---|---|---|---|---|
| A.5.1.2 Review of the policies for information security<br><br>The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | On cursory review of the policies and procedures showed there is no date of publication, history of maintenance and document owner. ISO27002 guidance requires policies and procedures to be subjected to periodic maintenance (review and update) by the document owner in partnership with SMEs.<br><br>No periodic review and maintenance of P&Ps and no policy owner approved management with responsibility for the development, review and evaluation of the policies. | ◐ | Include Document ownership and history of maintenance in each of the policies. | Low |

# Example 10 from an ISO 27002 Audit



# *Some Cybersecurity Compliance Frameworks*

**ISO 27001**
**NIST Cybersecurity Framework**
**DoD CMMC**
**Fed RAMP**
**CCPA**
**GDPR**
**AICPA SOC 2**
**SOX**
**PCI DSS**
**NY DFS Cybersecurity Regulation**
**FISMA**
**COBIT**
**CSA CSM**
**HIPAA**

# *Understanding Security Costs Vs. the Value of Information Assets & Nature of Inherent Risks*

| Medusa Corporation | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Threat Event** | **Cost of Control** | **Type of Control** | **ALE Before Application of Control** | **ALE After Application of Control** | **Cost Benefit Analysis** | **Worth the Cost?** | **Alternative Control if Not Worth the Cost** | **Agree with Analysis?** | **Agree with Recommended Alternative Controls?** | **Comments** |
| Programmer Mistakes | $20,000 | Training | $260,000 | $60,000 | $180,000 | Yes | | Yes | Not Applicable | |
| Loss of Intellectual Property | $15,000 | Firewall/IDS | $75,000 | $37,500 | $22,500 | Yes | | Yes | Not Applicable | |
| Software Piracy | $30,000 | Firewall/IDS | $26,000 | $6,000 | -$10,000 | Yes | Training | Yes | Yes | |
| Theft of Information (External) | $15,000 | Firewall/IDS | $10,000 | $5,000 | -$10,000 | Yes | | Yes | Not Applicable | Worth the negative CBA because the losses could be worse. |
| Theft of Information (Internal) | $15,000 | Phys. Security | $10,000 | $5,000 | -$10,000 | Yes | | Yes | Not Applicable | Worth the negative CBA because the losses could be worse. |
| Web Defacement | $10,000 | Firewall | $6,000 | $2,000 | -$6,000 | Yes | | Yes | Not Applicable | Worth the negative CBA because the losses could be worse. |
| Theft of Equipment | $15,000 | Phys. Security | $5,000 | $2,500 | -$12,500 | Yes | | Yes | Not Applicable | Worth the negative CBA because the losses could be worse. |
| Viruses, Worm, Trojan Horses | $15,000 | Antivirus | $78,000 | $18,000 | $45,000 | Yes | | Yes | Not Applicable | |
| DoS Attack | $10,000 | Firewall | $10,000 | $5,000 | -$5,000 | Yes | | Yes | Not Applicable | Worth the negative CBA because the losses could be worse. |
| Earthquake | $5,000 | Insurance/Backup | $12,500 | $12,500 | -$5,000 | Yes | | Yes | Not Applicable | Worth the negative CBA because the losses could be worse. |
| Flood | $10,000 | Insurance/Backup | $25,000 | $5,000 | $10,000 | Yes | | Yes | Not Applicable | |
| Fire | $10,000 | Insurance/Backup | $50,000 | $10,000 | $30,000 | Yes | | Yes | Not Applicable | |

# *Understanding the Return on Security Investment (RoSI)*

Return of Security Investment (RoSI) is an extremely important concept because most organizations operate with a budget hat is based on finite monetary resources.

However, the original RoSI models for Cybersecurity were based on concepts borrowed heavily from the ***Insurance Industry***, where losses were expected and even accepted as a matter of doing business.

Such thinking is not applicable in a scenario where a huge data breach can put an organization out of business, and likely negatively impact millions of people.


These formulas were actually on my CISSP exam when I took it in 2004

# *Understanding the Return on Security Investment (RoSI)*

**Phase 1: Impact Analysis**

To determine the impact of a new security program, we analyze our cyber-attack data before implementing the program to establish an initial incident trend baseline. Our analysis includes incident trends showing:

- Days between incidents: equivalent to the mean time between failures (MTBF) metric in the operations world
- Total incidents per year: annual rate of occurrence
- Breakdown by computing environments, volatility, and specific products

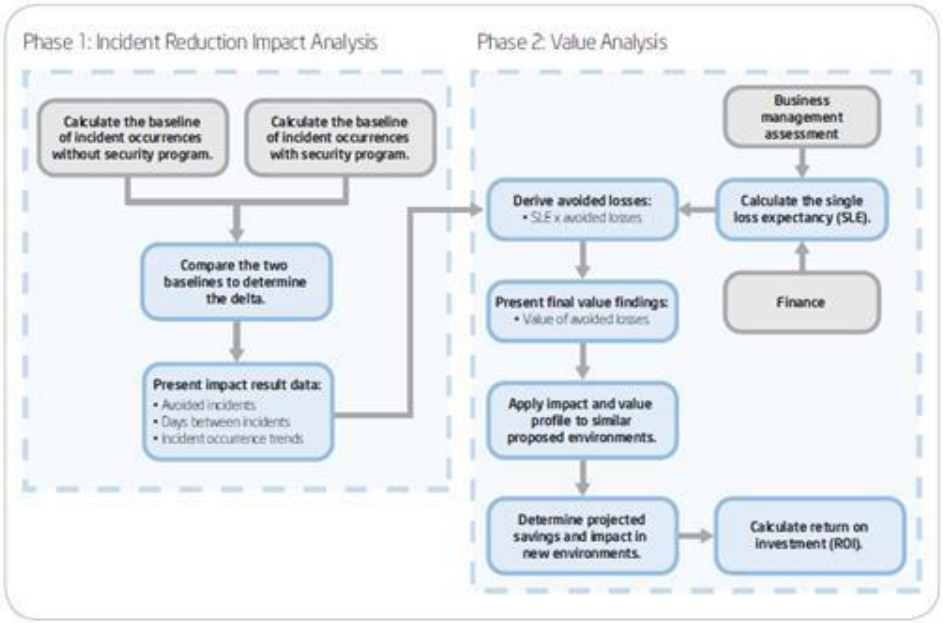



**Figure 2. Process for evaluating return on security investment (ROSI).** Actual incident data quantifies the impact in terms of reduced cyber-attacks and provides the basis for calculating the value of a security program.

Source: Intel Corporation Whitepaper: Measuring the Return on IT Security Investments, December 2007

**This is yet another view of RoSI. There are many versions of RoSI. The BEST RoSI is the one that best helps your Sr. Leadership & Board of Directors understand:**

**1) The levels of Cybersecurity possible and the value for the Budget Resources they allocate.**

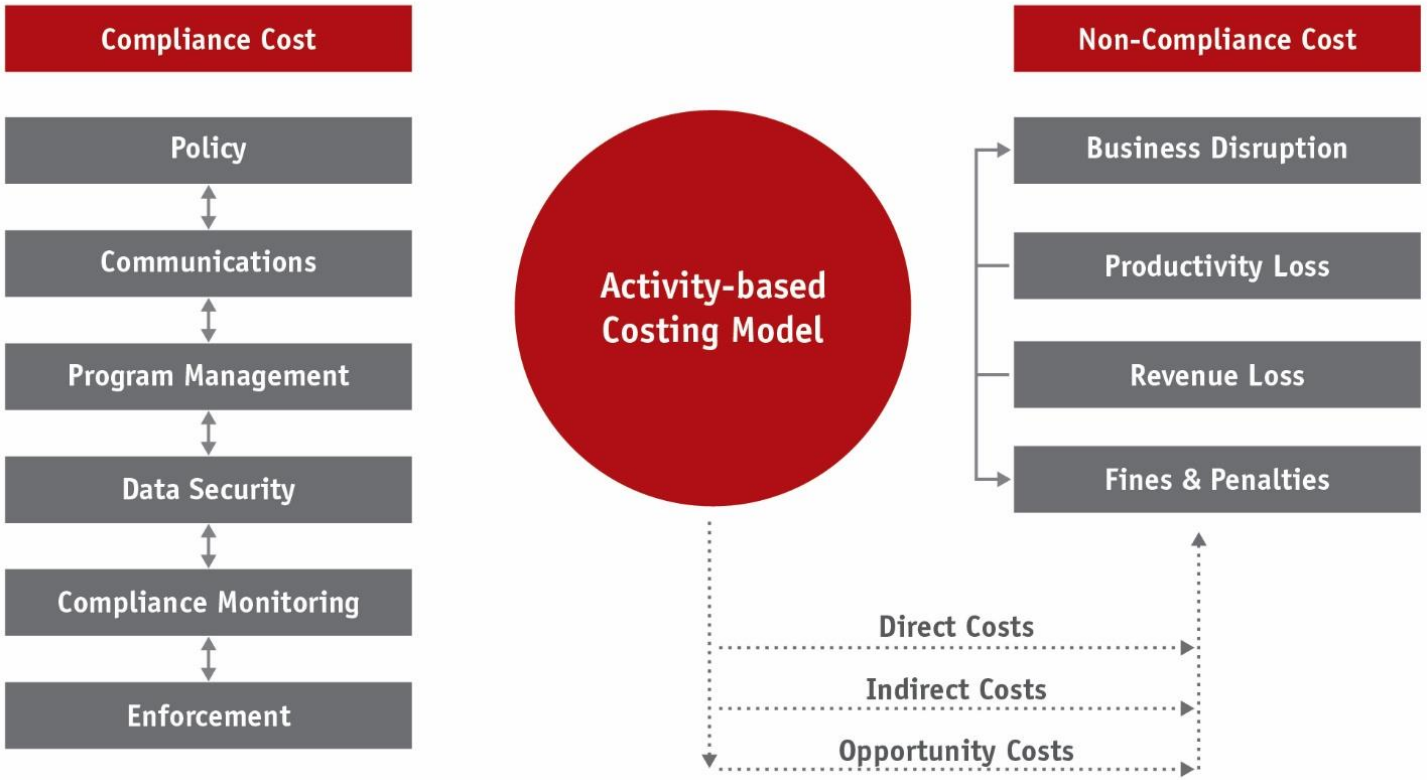
**2) That the organization is as secure as possible from breaches, fines, and brand damage.**

**3) They want to stay out of the Wall Street Journal, the New York Times, the Washington Post, the Internet, & the Verizon Annual DBIR.**

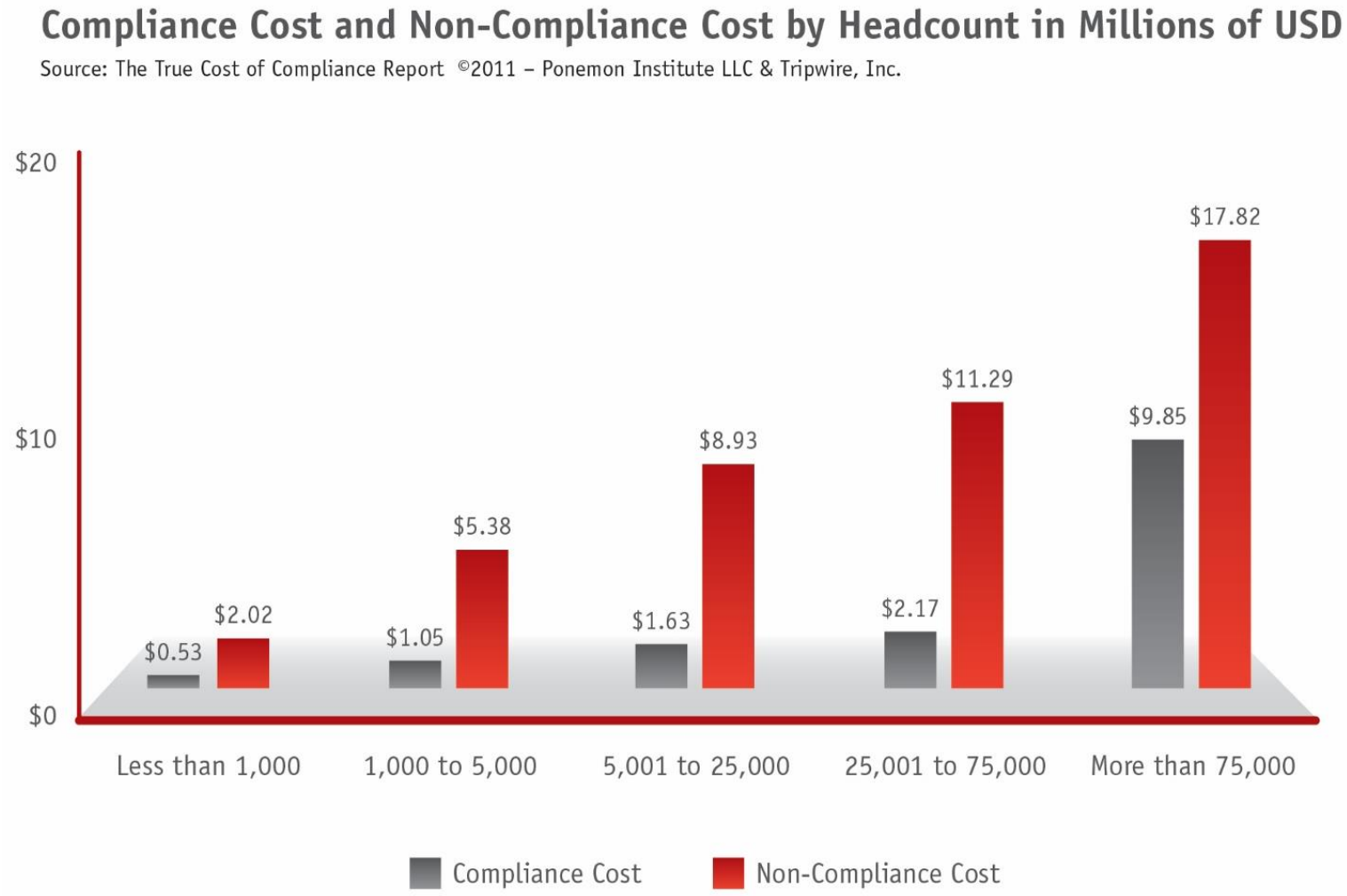
# Costs of Compliance Vs. Non-Compliance

## Total Compliance Cost Framework

Source: The True Cost of Compliance Report ©2011 – Ponemon Institute LLC & Tripwire, Inc.



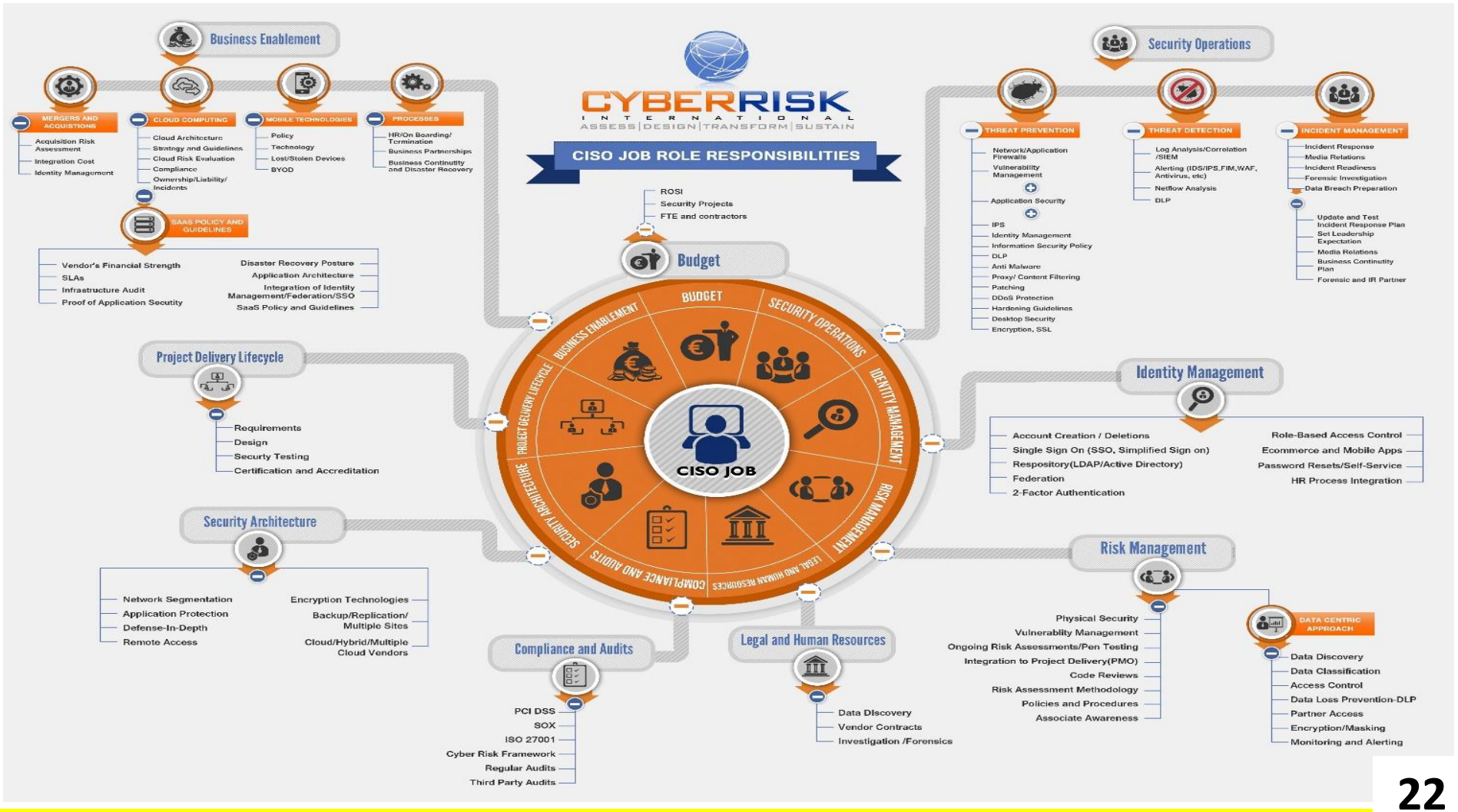
# Costs of Compliance Vs. Non-Compliance




**Bottom Line:**

**It's more prudent and cost effective to adopt and maintain a Cybersecurity Compliance Program.**

# Build a Strong Cybersecurity Leadership Team for Your Cybersecurity Management Program



# CISO MIND MAP v. 1.0

## Security Operations

- Prevention
  - Data Protection
    - Encryption, PKI, TLS
    - Data Loss Prevention (DLP)
    - Email Security
  - Network Security
    - Firewall, IDS/IPS, Proxy Filtering
    - VPN, Security Gateway
    - DDoS Protection
  - Application Security
    - Threat Modeling
    - Design Review
    - Secure Coding
    - Static Analysis
    - Web App Scanning
    - WAF, RASP
  - Endpoint Security
    - Antivirus, Anti-malware
    - HIDS/HIPS, FIM
    - App Whitelisting
  - Secure Configurations
  - Active Defense
  - Patching
- Detection
  - Log Management/SIEM
  - Continuous Monitoring
  - Network Security Monitoring
  - NetFlow Analysis
  - Advanced Analytics
  - Threat Hunting
  - Penetration Testing
  - Red Team
  - Vulnerability Scanning
  - Human Sensor
  - Data Loss Prevention (DLP)
  - Security Operations Center (SOC)
  - Threat Intelligence
  - Threat Information Sharing
  - Industry Partnerships
- Response
  - Incident Handling Plan
  - Breach Preparation
  - Tabletop Exercises
  - Forensic Analysis
  - Crisis Management
  - Breach Communications

## Legal and Regulatory

- Compliance
  - PCI
  - SOX
  - HIPAA
  - FFIEC, CAT
  - FERPA
  - NERC CIP
  - NIST SP 800-37 and 800-53
- Privacy
  - Privacy Shield
  - EU GDPR
- Audit
  - SSAE 16
  - SOC 2
  - ISO 27001
  - FISMA and FedRAMP
  - NIST SP 800-53A
  - COSO
- Investigations
  - eDiscovery
  - Forensics
- Intellectual Property Protection
- Contract Review
- Customer Requirements
- Lawsuit Risk

## Business Enablement

- Product Security
  - Secure DevOps
  - Secure Development Lifecycle
  - Bug Bounties
  - Web, Mobile, Cloud AppSec
- Cloud Computing
  - Cloud Security Architecture
  - Cloud Guidelines
- Mobile
  - Bring Your Own Device (BYOD)
  - Mobile Policy
- Emerging Technologies
  - Internet of Things (IoT)
  - Augmented Reality (AR)
  - Virtual Reality (VR)
- Mergers and Acquisitions
  - Security Due Diligence

CYBER LEADER

## Identity and Access Management

- Provisioning/Deprovisioning
- Single Sign On (SSO)
- Federated Single Sign On (FSSO)
- Multi-Factor Authentication
- Role-Based Access Control (RBAC)
- Identity Store (LDAP, ActiveDirectory)

## Risk Management

- Risk Management Frameworks
- Risk Assessment Methodology
- Business Impact Analysis
- Risk Assessment Process
- Risk Analysis and Quantification
- Security Awareness
- Vulnerability Management
- Vendor Risk Management
- Physical Security
- Disaster Recovery (DR)
- Business Continuity Planning
- Policies and Procedures
- Risk Treatment
  - Mitigation Planning, Verification
  - Remediation, Cyber Insurance

## Governance

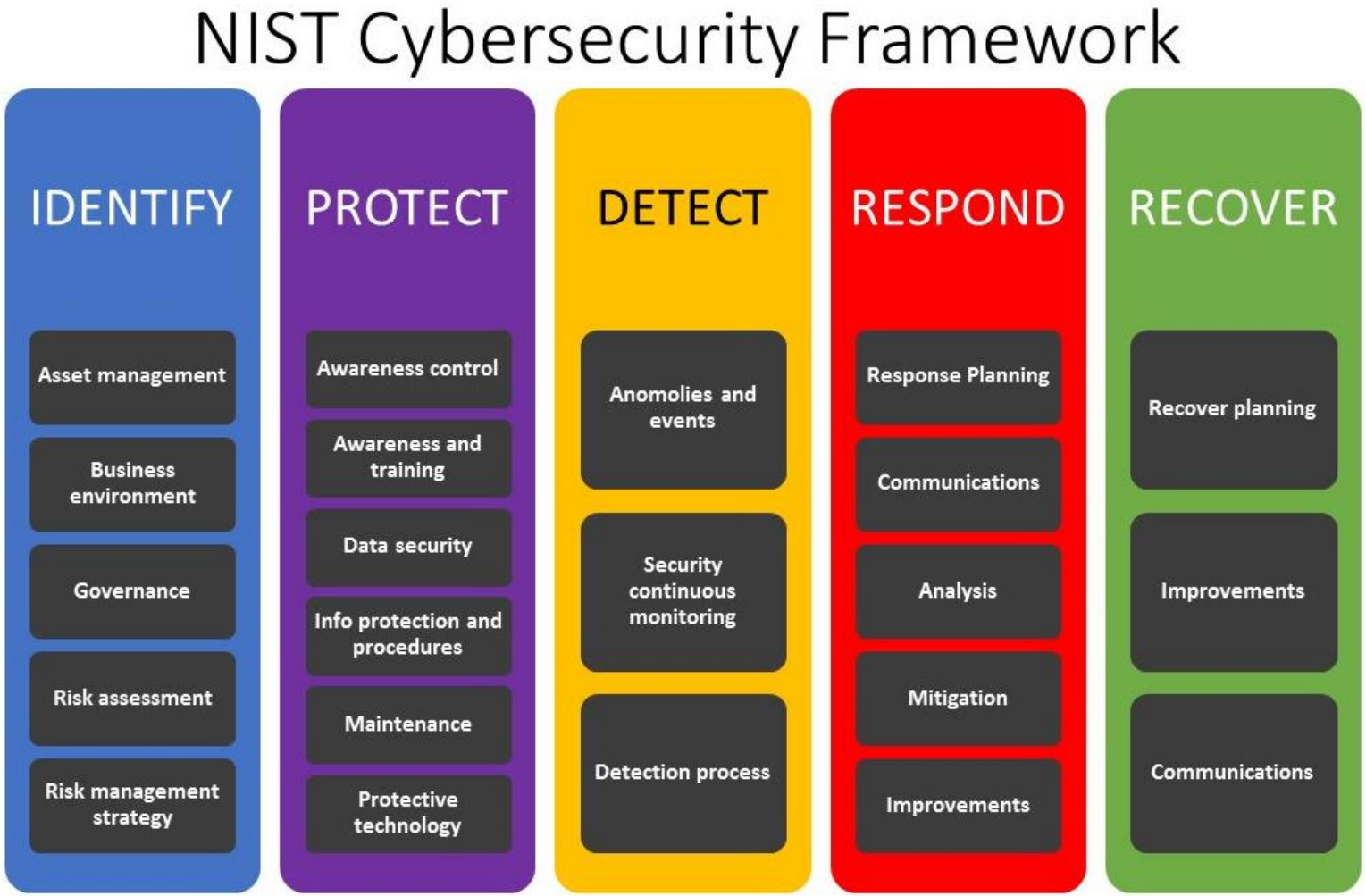
- Strategy
- Business Alignment
- Risk Management
- Program Framework
  - NIST CSF
  - ISO 27000
- Control Frameworks
  - NIST 800-53
  - Critical Security Controls (CSC)
- Program Structure
- Program Management
- Communications Plan
- Roles and Responsibilities
- Workforce Planning
- Resource Management
- Data Classification
- Security Policy
- Creating a Security Culture
- Security Training
  - Awareness Training
  - Role-Based Training
- Metrics and Reporting
- IT Portfolio Management
- Change Management
- Board Communications

## Leadership Skills

- Business Strategy
- Industry Knowledge
- Business Acumen
- Communication Skills
- Presentation Skills
- Strategic Planning
- Technical Leadership
- Security Consulting
- Stakeholder Management
- Negotiations
- Mission and Vision
- Values and Culture
- Roadmap Development
- Business Case Development
- Project Management
- Employee Development
- Financial Planning
- Budgeting
- Innovation
- Marketing
- Leading Change
- Customer Relationships
- Team Building
- Mentoring

*Based on CISO MindMap by Rafeeq Rehman @rafeeq_rehman http://rafeeqrehman.com Used v*

# *Select the Cybersecurity Framework for Your Cybersecurity Management Program*



# *Many Choose NIST Cybersecurity Framework for Their Cybersecurity Management Program*

| Functions | Categories |
|---|---|
| IDENTIFY (ID) | Asset Mangement (AM) |
| | Business Environment (BE) |
| | Governenace (GV) |
| | Risk Assessment (RA) |
| | Risk Management Stategy (RM) |
| PROTECT (PR) | Access Control (AC) |
| | Awareness and Training (AT) |
| | Data Security (DS) |
| | Information Protection Processess and Procedures (IP) |
| | Maintenance (MA) |
| | Protective Technology (PT) |
| DETECT (DE) | Anomolies and Events (AE) |
| | Security Continuos Monitoring (CM) |
| | Detection Processes (DP) |
| RESPOND (RS) | Incident Response Planning (RP) |
| | Communications (CO) |
| | Analysis (AN) |
| | Mitigation (MI) |
| | Improvements (IM) |
| RECOVER (RC) | Recovery Planning (RP) |
| | Improvements/Gap Remediation (IM) |
| | Communications (CO) |

# *Select the Cybersecurity Framework for Your Cybersecurity Management Program*

The NIST Cybersecurity Framework is popular because it

- **Helps reduce CyberRisk in a structured, well-designed manner**
- **Is proven**
- **Is Free**

## Cyber Security Framework

| Functions | Categories |
|---|---|
| IDENTIFY (ID) | Asset Mangement (AM) |
| | Business Environment (BE) |
| | Governenace (GV) |
| | Risk Assessment (RA) |
| | Risk Management Stategy (RM) |
| PROTECT (PR) | Access Control (AC) |
| | Awareness and Training (AT) |
| | Data Security (DS) |
| | Information Protection Processess and Procedures (IP) |
| | Maintenance (MA) |
| | Protective Technology (PT) |
| DETECT (DE) | Anomolies and Events (AE) |
| | Security Continuos Monitoring (CM) |
| | Detection Processes (DP) |
| RESPOND (RS) | Incident Response Planning (RP) |
| | Communications (CO) |
| | Analysis (AN) |
| | Mitigation (MI) |
| | Improvements (IM) |
| RECOVER (RC) | Recovery Planning (RP) |
| | Improvements/Gap Remediation (IM) |
| | Communications (CO) |

What processes and assets need protection?

How are we protecting our networks and data?

What are our capabilities for detecting a cyber attack?

What are our capabilities for responding to an attack?

What are our capabilities for returning to normal operations?

# *Build the Capability Maturity Model Roadmap of Your Cybersecurity Management Program*

## Cybersecurity Maturity Model Certification (CMMC)

The CMMC model consists of 17 domains. The majority of these CMMC domains originated from the FIPS 200 security-related areas and the NIST SP 800-171 control families. The CMMC model also includes the Asset Management, Recovery, and Situational Awareness domains.

These domains are shown in Figure 3 with their abbreviations as used in the model practice numbering system.

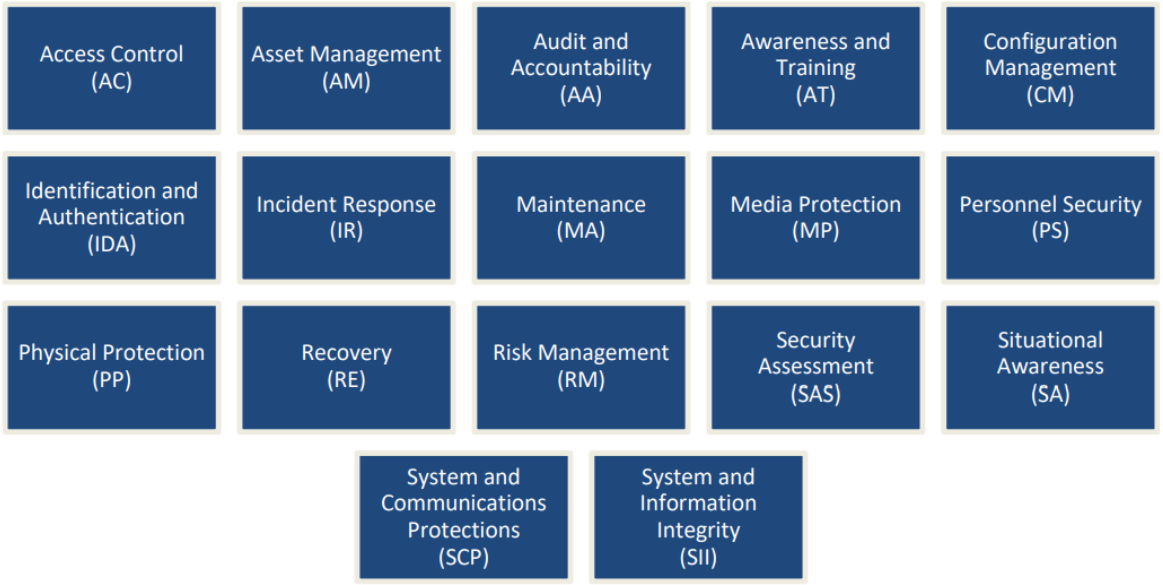
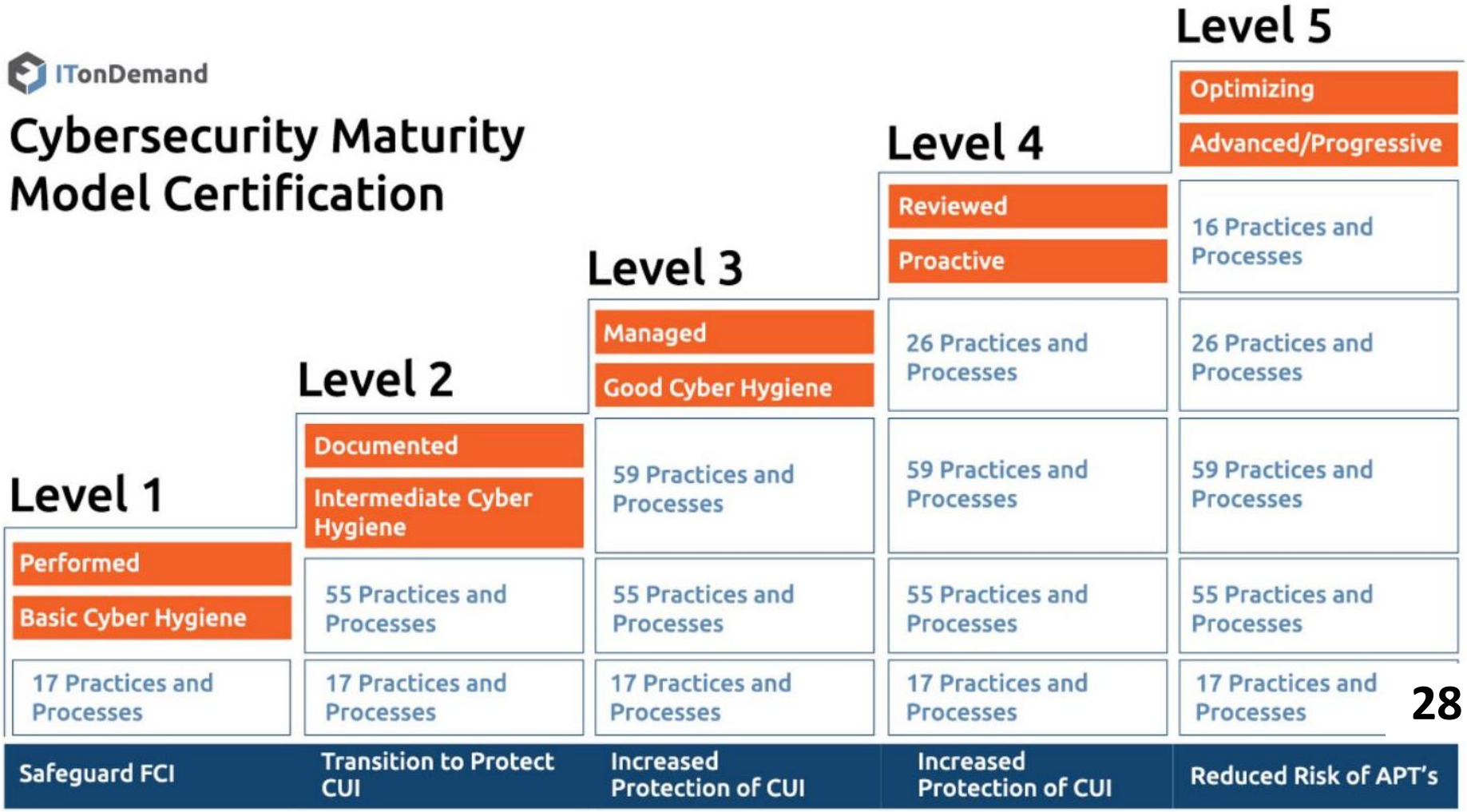



**Figure 3. CMMC Model Domains**

# *Build the Capability Maturity Model Roadmap of Your Cybersecurity Management Program*



# *Build the Capability Maturity Model Roadmap of Your Cybersecurity Management Program*

Cybersecurity Maturity Model Certification (CMMC)

## Model Rev 0.4 Synopsis - Practices

| | Description of Level Practices | CMMC Rev 0.3 Practices | New CMMC Rev 0.4 Material | CMMC Rev 0.4 Practices | Mapping: Controls |
|---|---|---|---|---|---|
| CMMC Level 1 | Basic Cyber Hygiene | 17 | +18 practices | 35 | FAR 52 |
| CMMC Level 2 | Intermediate Cyber Hygiene | 46 | +69 practices | 115 | |
| CMMC Level 3 | Good Cyber Hygiene | 63 | +28 practices | 91 | NIST SP 800-171 rev 1 |
| CMMC Level 4 | Proactive | 10 | +85 practices | 95 | NIST SP 800-171 rev B |
| CMMC Level 5 | Advanced / Progressive | 4 | +30 practices | 34 | |

### RE-CERTIFICATION PERIODS

Level 1 – 3 Years

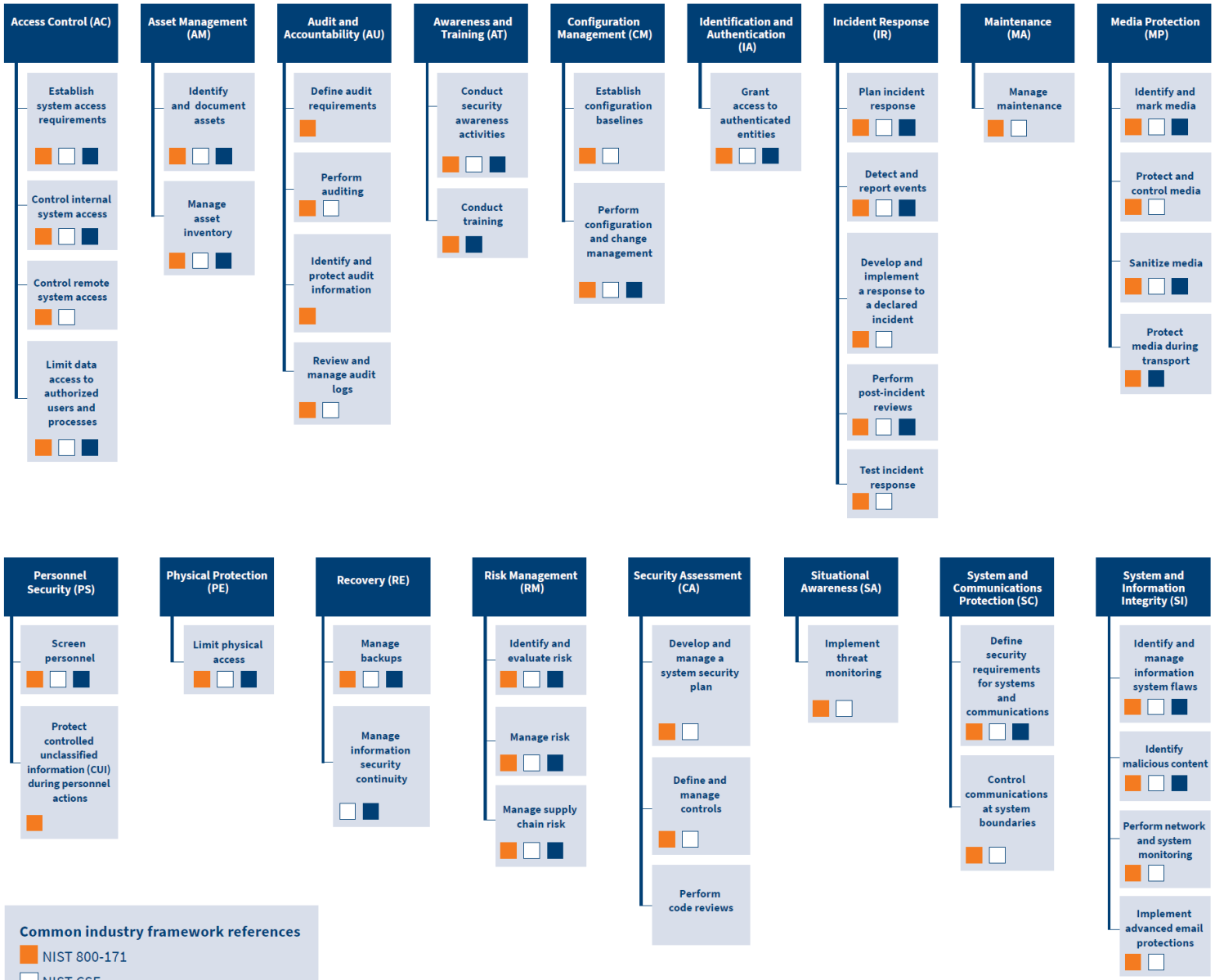
Level 2 – 3 Years

Level 3 – 2 Years

Level 4 – Annually

Level 5 – Annually

# THE 17 CMMC CYBERSECURITY CAPABILITY DOMAINS




CohnReznick
ADVISORY · ASSURANCE · TAX

# *Create and Operate Both a Vulnerability Management Program and Threat Management Program*

# *Baseline Your Cybersecurity Program*

Make sure you have chosen the Cybersecurity Management Framework that your organization can and will commit to

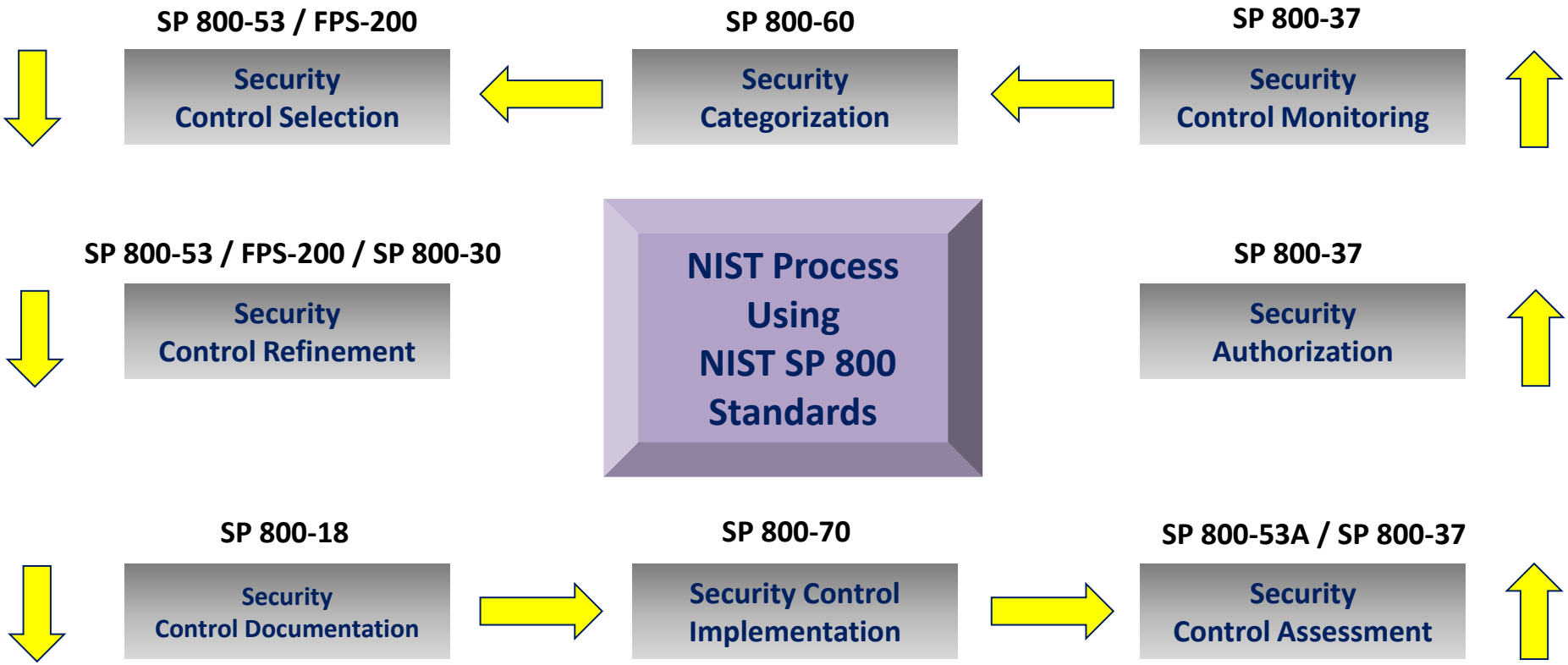
Ensure that you have Sr. Management Commitment and Support ***(Written is best.)***

Develop or use a pre-existing to tool to perform a ***Gap Analysis***.

Use the results of the ***Gap Analysis*** to
***Report the Present State of your Cybersecurity Management Program (your Baseline)***
Work with Senior Management to:

- Determine the Organizational needs and Budget Capacity to reduce **Inherent CyberRisk, the Levels of Risk Appetite and the Residual Risk**
- Create an Action Plan to Implement Better Cybersecurity and Achieve Required Levels of Inherent Risk Reduction
- Create the **Roadmap** to gradually Mature the Cybersecurity Program over time to better meet the Organization's Needs and adapt to the constantly evolving Cyberthreat Environment

# *Use Effective Cybersecurity Controls and Metrics AND Continuously Monitor & Measure*

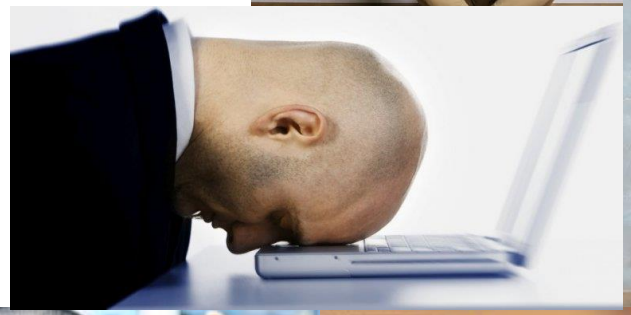


# *Hold Teams & Team Members Accountable*

Every Team, and Every Team Member should learn and adopt **Peter Senge Learning Team Disciplines:**

1. **Shared Vision**
2. **Personal Mastery**
3. **Mental Modeling**
4. **Team Learning**
5. **Systems Thinking**





# *Understand & Accurately Communicate the Current & Future Costs & Value of Your Cybersecurity Program*

Businesses run on money and ideas.

Business Unit Performance is usually measured in terms of profitability and meeting financial goals.

All items related to a Cybersecurity Management Program, people, processes, projects, programs, software, hardware, licenses, insurance, compliance costs, etc., have dollar values associated with each.

The seasoned Cybersecurity manager must understand all current costs that are enumerated in his or her Budget, and be accountable for these costs and the management of the resources. They must also well understand Risk Management and future costs and this often gets tricky, because future CyberThreats can be difficult to predict.

The Cybersecurity Manager will understand their Cybersecurity Management Program and all the resources associated with it, and understand how to articulate the true status of their program, its performance and challenges to Senior Management, who usually thinks in terms of Risk Management, Dollars, the Future Viability of the Organization, and staying out of Prison.

# Regularly Report the Results

## Stakeholder Concerns

| Stakeholders' Perspectives | Key Questions |
|---|---|
| Board of Directors<br>Executive Management Committee | What value does IT provide?<br>Does IT enable or retard growth?<br>Does IT advance organizational innovation & learning?<br>Is IT well managed? |
| Line of Business Management<br>Customer | Are we getting value for our IT investments?<br>How does IT influence the customer experience?<br>Does IT favourably affect productivity?<br>Is IT positioning us for future market demands? |
| Audit and Regulatory | Are the organization's assets and operations protected?<br>Are the key business and technology risks being managed?<br>Are proper processes and controls in place? |
| IT Organization | Are we doing the right things?<br>Are we effective?<br>Where do we need to improve to meet our goals?<br>Have we satisfied all key stakeholder interests?<br>Can we attract/retain the talent we need? |

Saull, R. (2013). The IT Balanced Scorecard: A Roadmap to Effective Governance of a Shared Services IT Organization. Retrieved from http://isaca.org on January 31, 2013.

# Regularly Report the Results


**Executive Report from 2007**

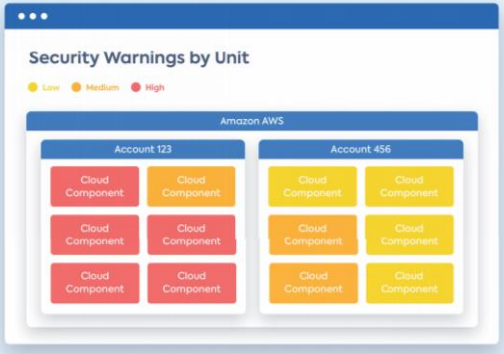
Figure 6: Enterprise Security Executive Report

# Regularly Report the Results

**CLOUD SECURITY AND COMPLIANCE**

**Executive Report from 2020**

C C R O V S




Which account and/ or subscription owner is responsible for mitigating security warnings?


How has the number of warnings evolved over time and how are they distributed among the different warning types?


What kind of violations affect my IT landscape?


Which violations exist in each geographical region and what criticality class do the violations affect?

LeanIX

# Regularly Report the Results

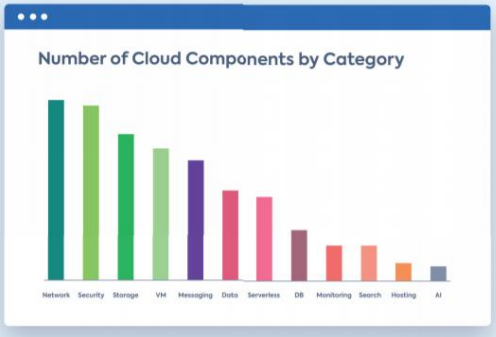
**Executive Report from 2020**

# Regularly Report the Results

**CLOUD PORTFOLIO MANAGEMENT**

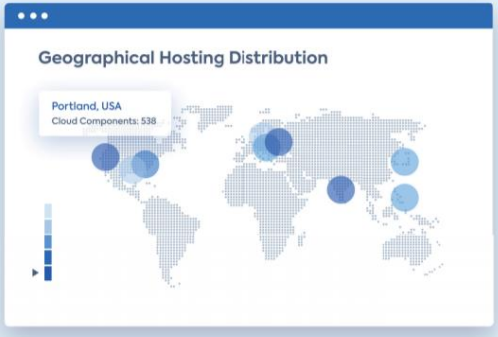
**Executive Report from 2020**

C C R O S

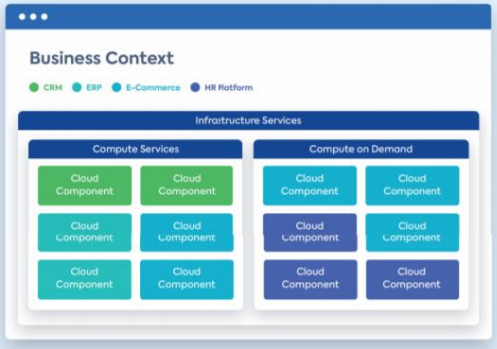



How many cloud components are in use by each category?


What is the distribution of cloud services in use?




How many cloud components are hosted in a region?

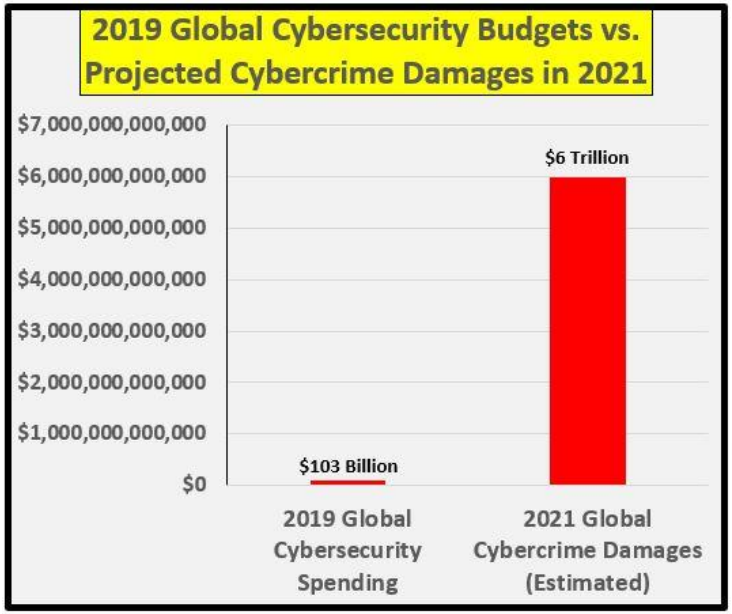



Which business service is supported by which cloud component and cloud component category?

LeanIX

# *Continuously Adapt & Grow*

- **The Bad Guys & their Threats far outnumber the Good Guys**
- **In 2019 Cybercrime was about an $880 Billion Industry**
- **In 2021, Cybercrime will be about a *$6 Trillion* Industry**
- **Continuous Adaptation and Growth are the only ways to survive as a Cybersecurity Professional**





Sources:
2017 Cybercrime Report by the Herjavic Group - https://www.herjavecgroup.com/resources/the-2017-cybercrime-report/
ZDNet - https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-idc/

Graphics:
William Favre Slater, III
slater@billslater.com

# Conclusion

In this short presentation, we covered the concepts of:

- Principles of Cybersecurity & Cybersecurity Management
- Cybersecurity Compliance Audit
- Cybersecurity Frameworks, their benefits and how to get started
- How to be Successful in Implementing and Managing a Cybersecurity Management Program
- Reporting the results to Senior Management

*Thank You!*

*Questions & Answers*

# Resources

# Resources

## DHS Cyber Security Offerings - CIOCC

**Cyber Hygiene Scanning (CyHy):**

- Broadly assess Internet-accessible systems for known vulnerabilities and configuration errors on a persistent basis.

**Phishing Campaign Assessment (PCA):**

- Measures susceptibility to email attack
- Delivers simulated phishing emails
- Quantifies click-rate metrics over a 6-week period

**Remote Penetration Testing (RPT):**

- Remote Penetration Test (RPT) utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways.

# Resources

## DHS Cyber Security Offerings - CSA

**Cyber Resiliency Review (CRR):**

- The Cyber Resilience Review (CRR) is a no-cost, voluntary, interview-based assessment to evaluate an organization's operational resilience and cybersecurity practices. (Strategic Report)

**External Dependencies Management Assessment (EDM):**

- The External Dependencies Management (EDM) assessment is a no-cost, voluntary, interview-based assessment to evaluate an organization's management of their dependencies. (Tactical Report)

**Cyber Infrastructure Survey (CIS):**

- The Cyber Infrastructure Survey (CIS) is a no-cost, voluntary survey that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience. (Operational Report)

# Resources


NCCIC 24x7 Duty Officer:
888-282-0870

Report incidents:
https://www.us-cert.gov/report

Contact watch and warning operations:
NCCIC@hq.dhs.gov

Find resources:
https://www.us-cert.gov/ccubedvp

Federal Bureau of Investigation:
www.ic3.gov

MS-ISAC
866-787-4772
soc@msisac.org

**Geoffrey Jenista, CISSP**
**Cybersecurity Advisor (CSA), Region VII (IA, KS, MO, NE)**
**Cyber Security Division**
Geoffrey.Jenista@cisa.dhs.gov
**913-249-1539**

# Resources

## RESOURCES

- www.secretservice.gov/contact/field-offices/ (United States Secret Service)
  - Chicago Field Office – 312-353-5431
  - Cleveland Field Office – 216-750-2058
  - Detroit Field Office – 313-226-6400
  - Indianapolis Field Office – 317-635-6420
- www.dhs.gov/be-cyber-smart (Department of Homeland Security)
- www.us-cert.gov (Cybersecurity & Infrastructure Security Agency)
- www.cisa.gov (Cybersecurity & Infrastructure Security Agency)

THE #CYBERAVENGERS
www.thecyberavengers.com

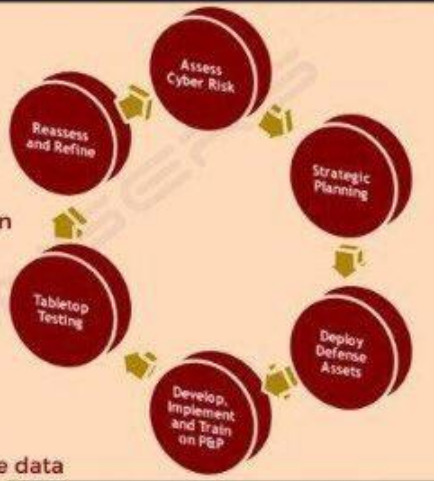
# Good Cyber Hygiene Checklist

- ☐ Start with a risk assessment
- ☐ Have written policies and procedures on:
  - ☐ Expectations for protecting data
  - ☐ Confidentiality of data
  - ☐ Expectations for privacy
  - ☐ Monitoring that impact privacy
  - ☐ Limits of permissible acces and use
  - ☐ Social engineering
  - ☐ Password policy and security questions
  - ☐ BYOD

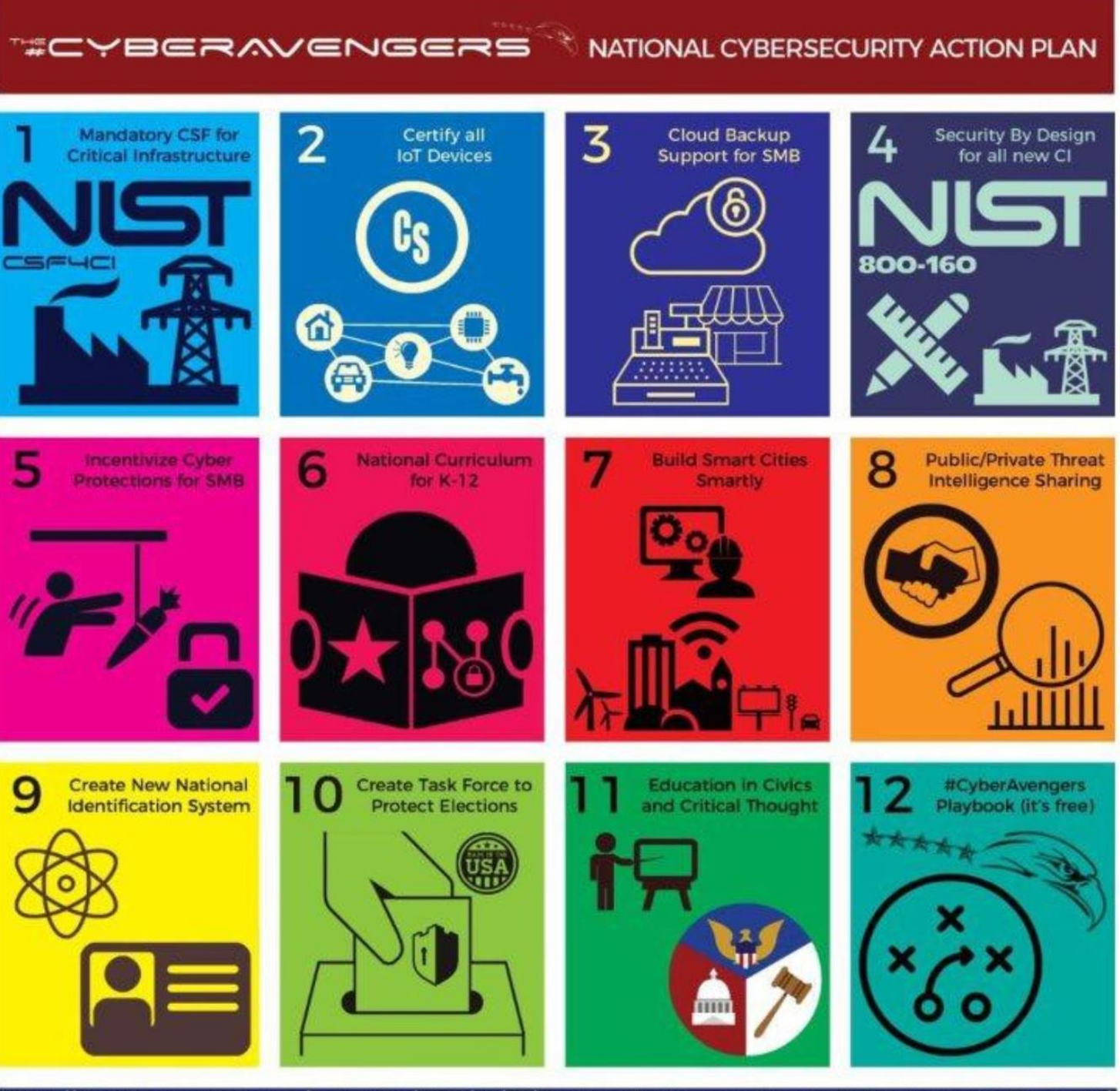
  * Make sure to tailor these to your company
- ☐ Training of all workforce on your policies and procedures, first, then security training
- ☐ Phish **all** workforce (upper management too!)
- ☐ Multi-factor authentication
- ☐ Signature based antivirus and malware detection
- ☐ Internal controls / access controls
- ☐ No default passwords
- ☐ No outdated or unsupported software
- ☐ Security patch updates management policy
- ☐ Backups: segmented offline, cloud, redundant
- ☐ Use reputable cloud services
- ☐ Encrypt sensitive data and air-gap hypersensitive data
- ☐ Adequate logging and retention
- ☐ Incident response plan
- ☐ Third-party security risk management program
- ☐ Firewall, intrusion detection, and intrusion prevention systems
- ☐ Managed services provider (MSP) or managed security services provider (MSSP)
- ☐ Cyber risk insurance

Cybersecurity breaches and their aftermath have been proven to be terminal events for C-Suite executives and present a dimension of existential risk to an organization, its revenues, earnings and reputation.

- The #CyberAvengers Playbook




If your IT department says to you, "we're confident we do not have any malware on our network" ask how they came to that conclusion. If instead they say, "we do not have any malware on our network, honest, trust us!" then raise an eyebrow and get your hands dirty, because you have work to do.


THE #CYBERAVENGERS
NATIONAL CYBERSECURITY ACTION PLAN
1
Mandatory CSF for Critical Infrastructure
NIST
CSF4CI
2
Certify all IoT Devices
3
Cloud Backup Support for SMB
4
Security By Design for all new CI
NIST
800-160
5
Incentivize Cyber Protections for SMB
6
National Curriculum for K-12
7
Build Smart Cities Smartly
8
Public/Private Threat Intelligence Sharing
9
Create New National Identification System
10
Create Task Force to Protect Elections
USA
11
Education in Civics and Critical Thought
12
#CyberAvengers Playbook (it's free)
https://thecyberavengers.com/index.php/2017/10/23/a-national-cybersecurity-action-plan-is-a-serious-priority/

svb

Silicon Valley Bank

Cybersecurity

# How Tech Companies Prepare for Cyber Attacks

**98%** Of small and mid-size technology and healthcare companies are maintaining or increasing resources devoted to cybersecurity this year, preparing for when, not if, cyber attacks occur.

**50%** Are increasing their spend, and investing in active response, not infrastructure.

## Most Common Cybersecurity Resource Investments

- Monitoring/Assessment **18%**
- Policies/controls **15%**
- Hiring **12%**
- Software **8%**
- Firewalls **8%**
- Authentication/Access **6%**
- Encryption **6%**

*Just* **35%** Are completely or very confident in the **security of their company information.**

**52%** Are storing their info **privately,** not in the public cloud.

**76%** Say cyber attacks **threaten serious business interruption.**

**54%** Of non-security companies have or plan to **add a cybersecurity** component to their product.

**46%** Say media attention has **increased awareness** of the issue.

**78%** Say their data and IP are **threatened.**

Statistics come from the results of an SVB survey about cybersecurity completed by 216 C-level executives from US-based technology and life science companies in July 2013. B-13-12992. Rev. 09-20-13

# Do You Know Cyber?
# Security Teams

The ingredients of an effective security team.

## Who is Recruited Into a Security Team

### Chief Executive
**CEO or Business Owner**
A mandate for security must start at the highest executive office. The CEO also sets the tone of a security culture.

### CISO
**Chief Info. Security Officer**
The ISO is responsible for strategic planning, as well as oversight and reporting on all security operations.

### Technologists
**AKA the IT Department**
Technologists play an important custodial role when it comes to care and maintenance of cyber assets.

### Management
**All of Management**
In today's digitized economy the role of asset principal (even if shared) is inherent to every management position.

### Security Talent
**White Hats and Friends**
A few cyber actions require special skills. Talent trained in cyber risk mgt. and operations are sometimes required.

**It common when the "security team" is mentioned to think of the technology department or perhaps a breed of super hacker technologist subculture.**

**Effective cyber security contrasts with this vision however with roles to be played by individuals across the organization.**

## How Team Members Relate to Assets

### Management
**All of Management**
Every manager sets cyber hygiene expectations for their staff. They also map threats and security requirements.

### Asset Owner
**AKA System Owner**
This individual holds overall responsibility for an asset. They probably bought it (or defined the requirements).

### Security Talent
**Engineers & Analysts**
Engineers and analysts are sometimes but not always required to maintain asset security.

### Data Steward
**The Data "Hall Monitors"**
Through various means, stewards review, update, monitor and manage data integrity when others can't.

### Asset Custodian
**Maintenance & Care**
Likely a technologist, this individual maintains and operates the asset from a technical perspective.

**A cyber asset is any component of a cyber digital (or information) system.**
**Examples:**

Endpoints:
- Phones or Tablets
- Desktop or Laptop PCs

Servers:
- Physical or Virtual
- A Server in the Cloud

Software:
- Installed on an Endpoint
- Software as a Service

Data:
- In a Database or a File
- Stored by Any Application

Managed:
- GMail, Dropbox or O365
- Your Cell Provider or ISP

Partners & Processors:
- Your Payment Processor
- Your Bank and Every Vendor

And don't forget door locks, printers, and industrial machinery.

## Security Stakeholders

### Business Owner
**CEO or Business Owner**
The highest executive office always has ultimate accountability for business risk -- this includes cyber risk.

### The Board
**Directors or Trustees**
Like any high profile business risk the board should be involved in overall security strategy and reporting.

### Asset Principals
**Owners, Custodians ...**
All cyber assets require ownership, care, maintenance and stewardship. Properly assigning these roles is critical.

### Auditors
**Inside or Outside Auditors**
Auditors provide a measure of objectivity in analyzing cyber risk and evaluating cyber security posturing.

### Data Steward
**The Data "Hall Monitors"**
Security Engineering can only go so far. Data Stewards make sure information in systems is accurate and useful.

### Underwriters
**Risk Transfer Agents**
Insurers provide price based incentives for good security, and help transfer difficult to manage risk.

### Security Talent
**Engineers & Analysts**
Cyber warriors armed with best practice and specialized skills. The special operators of any good security team.

### Regulators
**Protecting Common Good**
Government intervention is sometimes required when market incentives fail to protect the common good.

### Threat Actor
**The Bad Guys**
Whether they're criminals, insiders or hostile states -- there are many threat actors looking for security failures.

### End Users
**AKA, Normal People**
End Users are responsible for their own cyber hygiene, but ultimately they depend on the security team doing their part.

#doyouknowcyber

fortmesa.com/learn-sec-teams

FortMesa

# William Favre Slater, II


- 312-758-0307
- slater@billslater.com
- williamslater@gmail.com
- http://billslater.com/interview
- 1515 W. Haddon Ave., Unit 309
  Chicago, IL 60642
  United States of America


William Favre Slater, III



53

# Bellevue University

*By Charter of the State of Nebraska and upon the recommendation of the Faculty and Administration, the Board of Directors of Bellevue University authorizes the award of the*

## Master of Science in Cybersecurity

*degree to*

## William Faure Slater III

*in recognition of the fulfillment of the requirements for this degree with all the Rights, Privileges, and Responsibilities pertaining to it. In Testimony Thereto, we have subscribed our names, confirmed by the Seal of the University in Bellevue, Nebraska, this thirty-first day of March, 2013.*

George A. Little
Chair of the Board

BELLEVUE UNIVERSITY

Mary Hawkins
President

# International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

## William FAVRE Slater

the credential of

## Certified Information Systems Security Professional

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.

Jennifer Minella - Chairperson

Zachary Tudor - Secretary

CISSP®

ANSI Accredited Program PERSONNEL CERTIFICATION
ISO/IEC 17024

57707
Certification Number

Aug 1, 2019 - Jul 31, 2022
Certification Cycle

Certified Since: 2004

(ISC)²

Verify Member is in good standing at:www.isc2.org/verify

Printed On: 8/1/2019

# International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

## William FAVRE Slater

the credential of

## Systems Security Certified Practitioner

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.

Jennifer Minella - Chairperson

Zachary Tudor - Secretary

SSCP®

ANSI Accredited Program PERSONNEL CERTIFICATION

ISO/IEC 17024

57707

Certification Number

May 1, 2019 - Apr 30, 2022

Certification Cycle

Certified Since: 2004

(ISC)²

Verify Member is in good standing at:www.isc2.org/verify

Printed On: 8/1/2019

CISA® Certified Information Systems Auditor®

An ISACA® Certification

ISACA hereby certifies that

# WILLIAM SLATER

has successfully met all requirements and is qualified as **Certified Information Systems Auditor;**
in witness whereof, we have subscribed our signatures to this certificate.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISA continuing professional education policy; and passage of the CISA exam.

| 0976208 | 28 August 2009 | |
|---|---|---|
| Certification Number | Date of Certification | Chair, ISACA Board of Directors |
| | 31 January 2022 | |
| | Expiration Date | ISACA - Chief Executive Officer |

ISACA®

Trust in, and value from, information systems