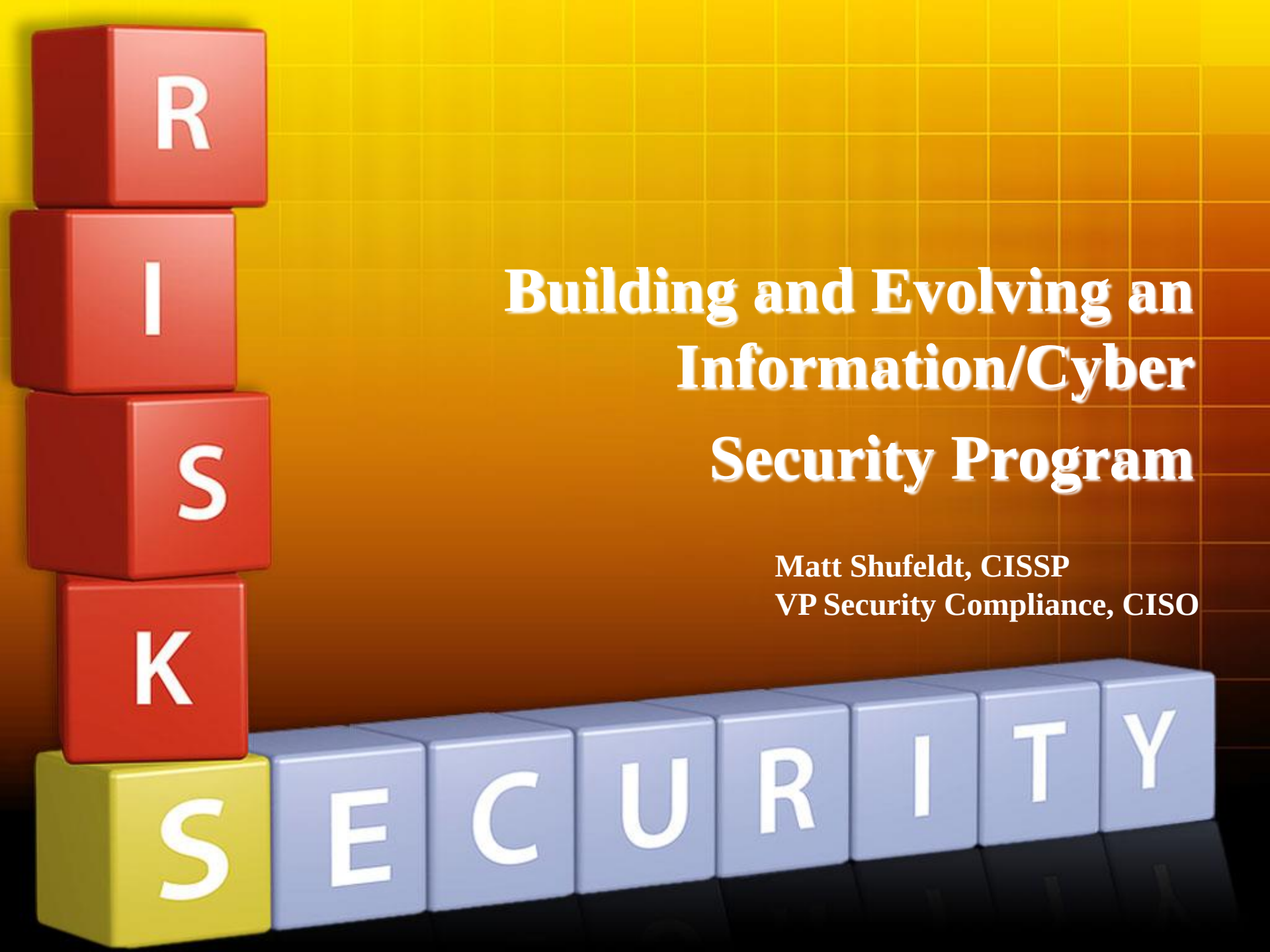


Building and Evolving an Information/Cyber Security Program

Matt Shufeldt, CISSP
VP Security Compliance, CISO

Setting the Stage

The 12 Information Security Principles

Support the business

1. Focus on the business
2. Deliver quality and value to stakeholders
3. Comply with relevant legal and regulatory requirements
4. Provide timely and accurate information on security performance
5. Evaluate current and future information threats
6. Promote continuous improvement in information security

Defend the business

7. Adopt a risk-based approach
8. Protect classified information
9. Concentrate on critical business applications
10. Develop systems securely

Promote responsible security behavior

11. Act in a professional and ethical manner
12. Foster a security-positive culture

*Note - Leading security organizations ISF, (ISC)²® and ISACA jointly launched these principles to govern behavior, objectives, approach and activities

Security Leader backgrounds

Technology

Business

Finance

Accounting

IT Service Management

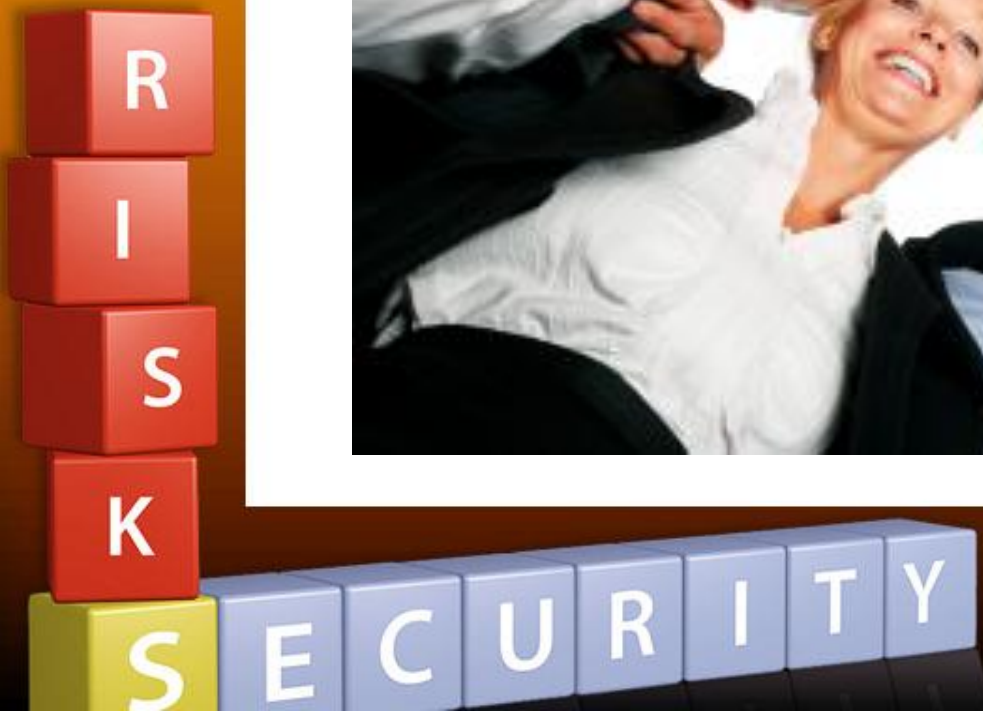
Risk Management

Governance/Audit

Legal

***Note - Leading security organizations ISF, (ISC)²® and ISACA jointly launched these principles to govern behavior, objectives, approach and activities**

It’s all about the team

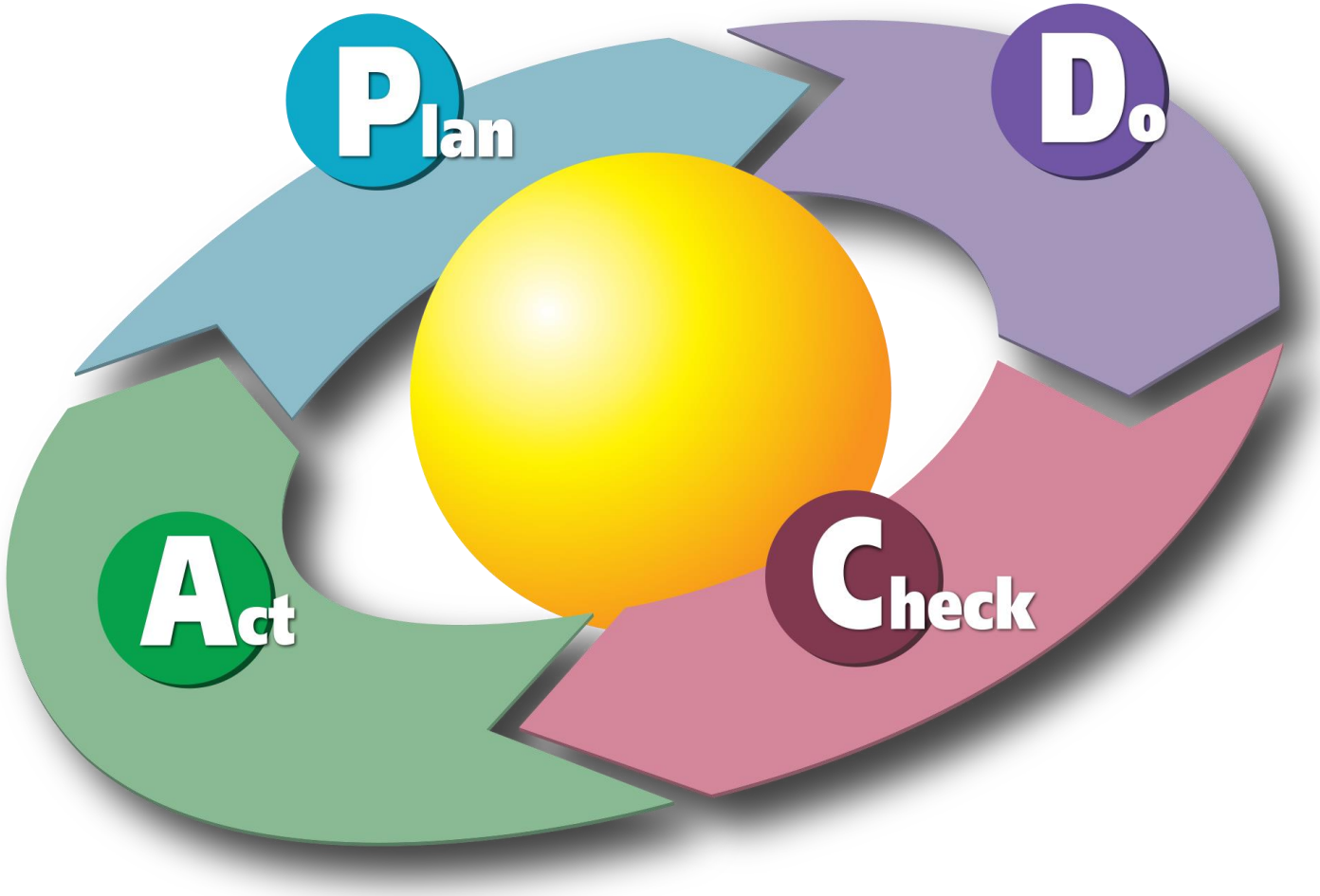


Diversity is the quickest road to well rounded

1. Assess your leaders and peers (direct, steering committee and oversight board)
2. Assess your team (direct and matrix)
3. Assess yourself
4. Be honest
5. Use this information for team development and hiring decisions

***Note - Leading security organizations ISF, (ISC)²® and ISACA jointly launched these principles to govern behavior, objectives, approach and activities**

PDCA



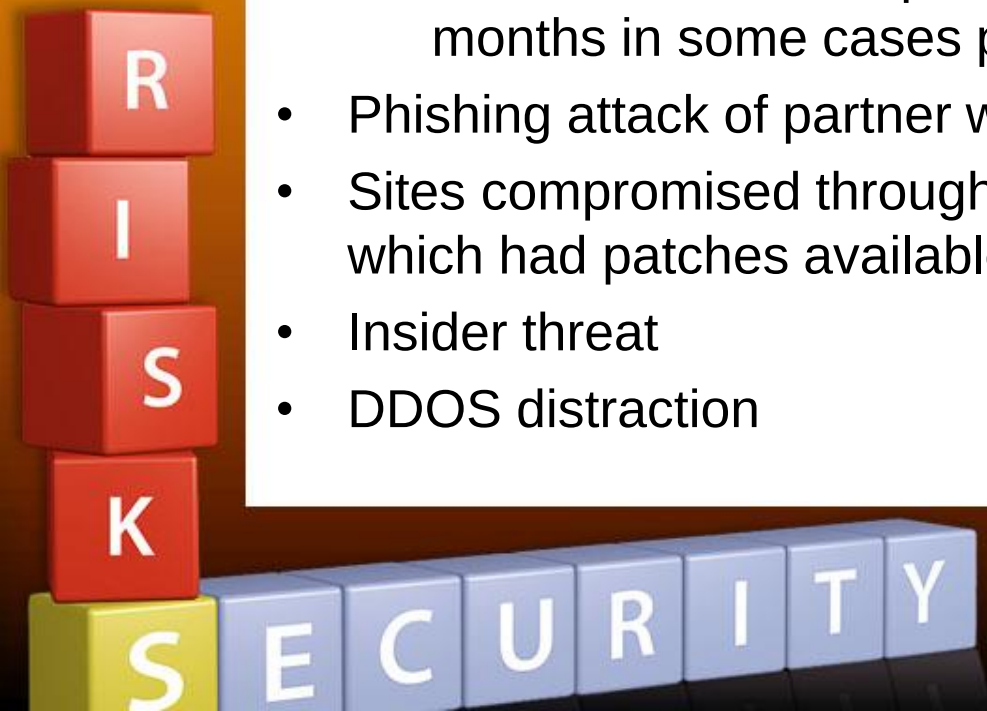
What has happened?

Looking back on the last few years we see some disturbing trends.

1. Insider threats
2. World wide significant security vulnerabilities
3. Massive DDOS attacks
4. Data breaches
5. Data breaches
6. And some more data breaches

Common Breach Approaches Utilized

- Malware
  - By far the most common culprit in play right now
  - Some strains appear to be polymorphic and have anti-forensic properties
  - Multiple strains are unsophisticated and were crudely customized for specific targets
  - Malware and corresponding actors were in environments for months in some cases prior to active theft (APT)
- Phishing attack of partner with access
- Sites compromised through known vulnerabilities many of which had patches available.
- Insider threat
- DDOS distraction



Contributing Factors

- Ineffective and sometimes incompetent security vendors
- Poor segmentation practices
- Lack of traffic monitoring and controls
- Poor data handling practices
- Lack of central responsibility and accountability for Information Security
- No action taken when “alarms” were triggered in some cases
- Regular patch management and maintenance not being performed

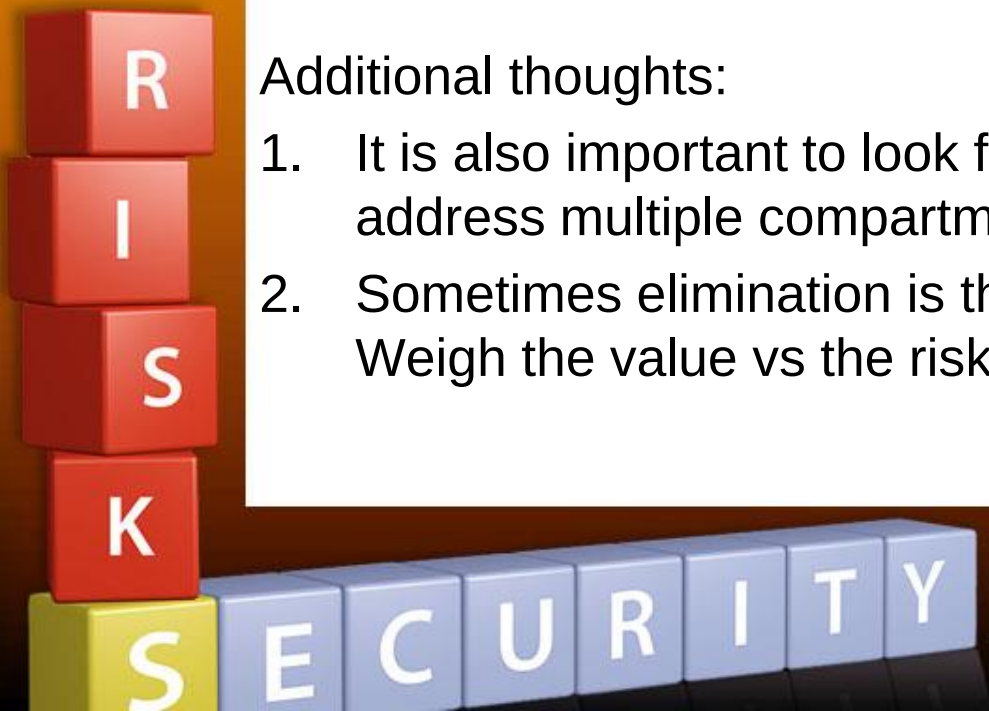
Where do we go from here?

Prioritization or is it triage?

1. Assess/Make Lists
2. Compartmentalize
3. Apply detective controls to plan step 4 for first compartment
4. Isolate utilizing preventative controls
5. Apply remaining detective controls
6. Pick next compartment and start at step 3 again

Additional thoughts:

1. It is also important to look for quick wins and steps that could address multiple compartments at once
2. Sometimes elimination is the best method for remediation. Weigh the value vs the risk with your business partners



Defense in Depth: Detection

<u>The Basics</u>

- Network/Host based IDS/IPS monitoring
- Network/Host based firewall monitoring
- File integrity monitoring
- Centralized log management and correlation
- Properly configured SIEM

<u>The Advanced</u>

- IOC data imported for use in the basic solutions
- Network analysis tools
- 0 day/APT detection
- Fully staffed and trained SOC
- Fully staffed and trained Incident Response Team
- Trained Hunters – Very advanced
- Security Intelligence – Very advanced
- Security Analytics – Very advanced

Defense in Depth: Prevention

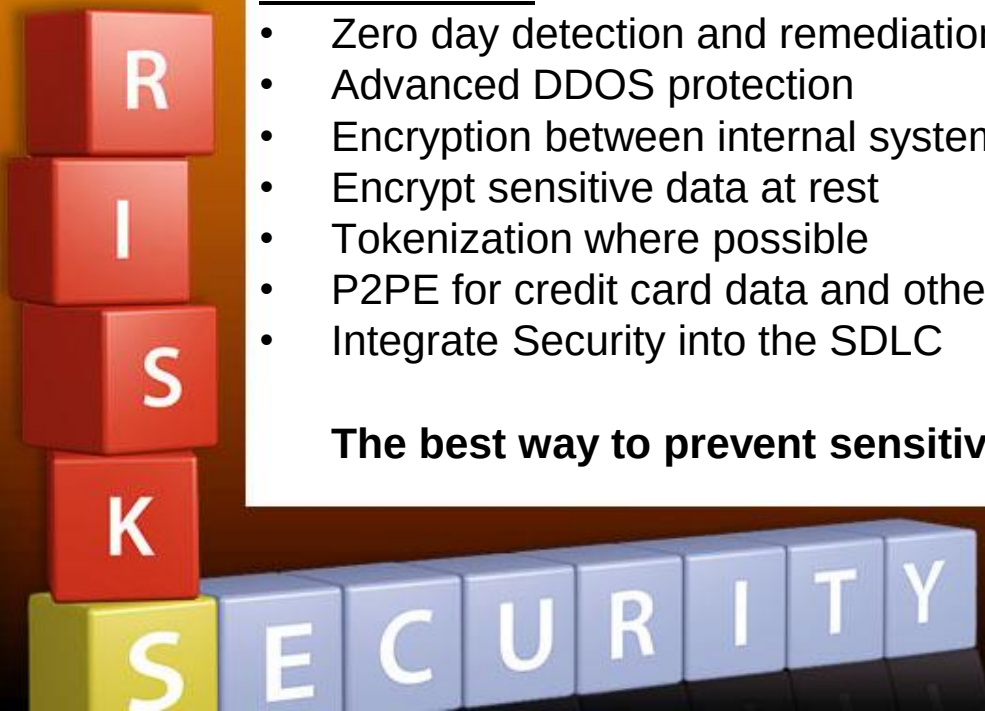
The Basics

- Harden clients and servers
- Integrate security into the Change Control process if not already present
- Data loss prevention
- Multiple layers of virus and malware protection
- Segment, segment, segment
- Encrypt sensitive data at rest
- Network/Host Firewalls and IDS/IPS

The Advanced

- Zero day detection and remediation tools
- Advanced DDOS protection
- Encryption between internal systems
- Encrypt sensitive data at rest
- Tokenization where possible
- P2PE for credit card data and other manageable data types
- Integrate Security into the SDLC

The best way to prevent sensitive data from being stolen is not to have it.

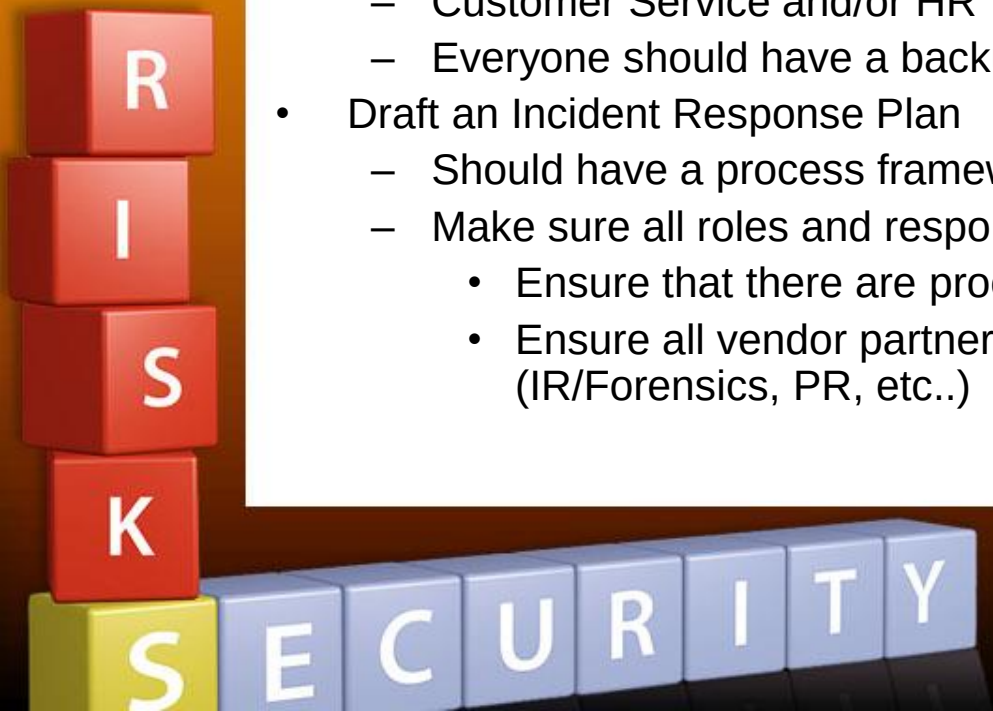


Incident Response

You should treat having a breach as an eventuality

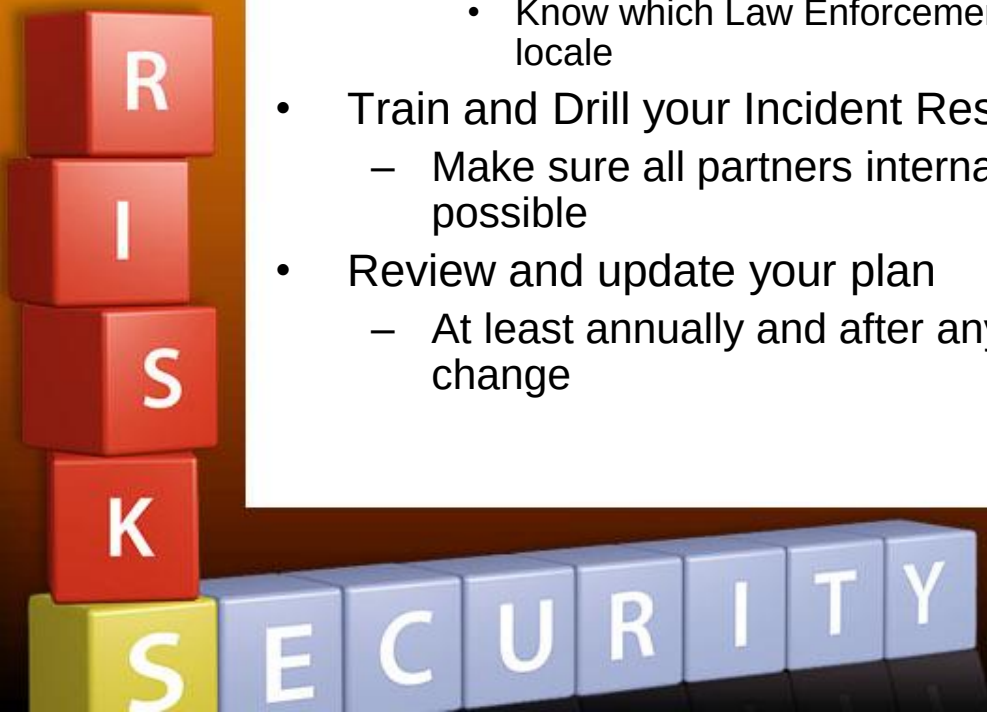
<u>Preparedness</u>

- Assemble an Incident Response Team
  - Lead – Normally your CISO, CPO or someone from Legal
  - IT and/or Information Security team member(s)
  - Legal
  - Marketing and/or PR
  - Customer Service and/or HR
  - Everyone should have a backup
- Draft an Incident Response Plan
  - Should have a process framework with key decision points
  - Make sure all roles and responsibilities needed are clearly defined
    - Ensure that there are procedures and/or scripts for each area
    - Ensure all vendor partners are defined and part of the plan (IR/Forensics, PR, etc..)



Incident Response continued

- Know your obligations for reporting and cooperating with Law Enforcement
  - Make sure you aren't put into any conflicts between these two or other entities
- Know your partners
  - Incident Response (IR) and Forensics partners
    - Negotiate this deal ahead of time and have the relationship established
  - PR firm
    - Ensure they know every reasonable scenario that could occur
  - Law Enforcement
    - Know which Law Enforcement partner(s) you should be using per scenario and locale
- Train and Drill your Incident Response Plan
  - Make sure all partners internal and external are involved whenever possible
- Review and update your plan
  - At least annually and after any major applicable business or technology change



Program Maturity: Security Lifecycle

<u>Self</u>

1) Fully Integrated Security into the SDLC
    1) Perform static code analysis
    2) Web/non-web application security testing
    3) System vulnerability testing based on hardening standards built on best practices
    4) Understand the total value and impact of open source solutions
2) Integrate Security into Enterprise Architecture
    1) Design reviews
    2) Data integration reviews
    3) Technology evaluations
3) Integrate Security into the PMO

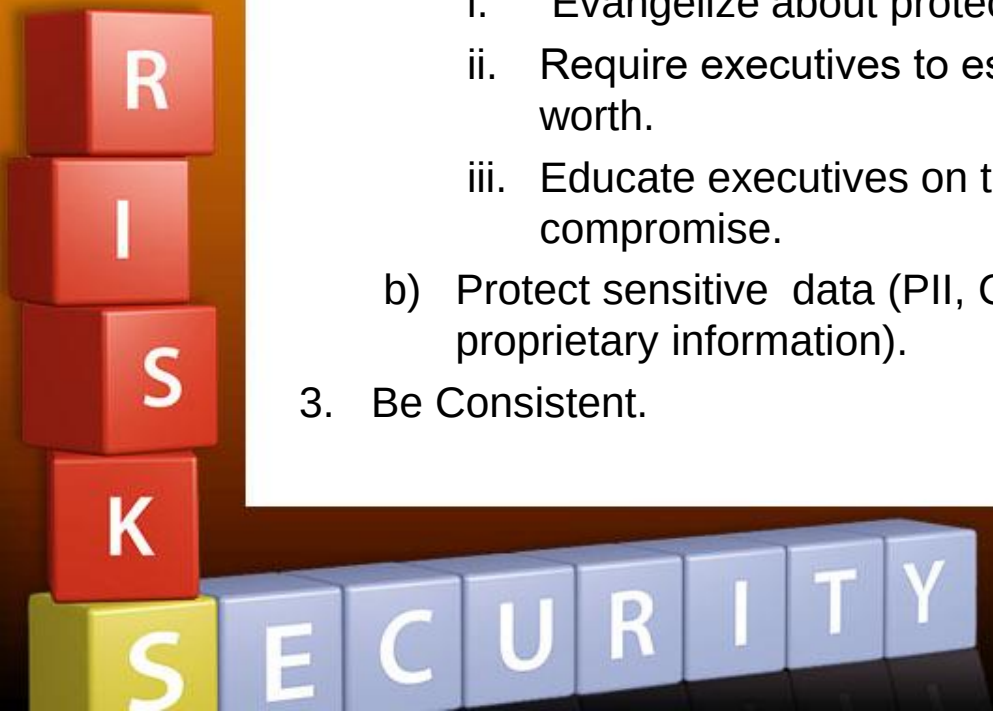
<u>Third Party Management</u>

1) Integrate Security into the Procurement/Contract process
2) Assess third parties based on risk, value and total investment
    1) Be careful not to overlook the partners of your partners

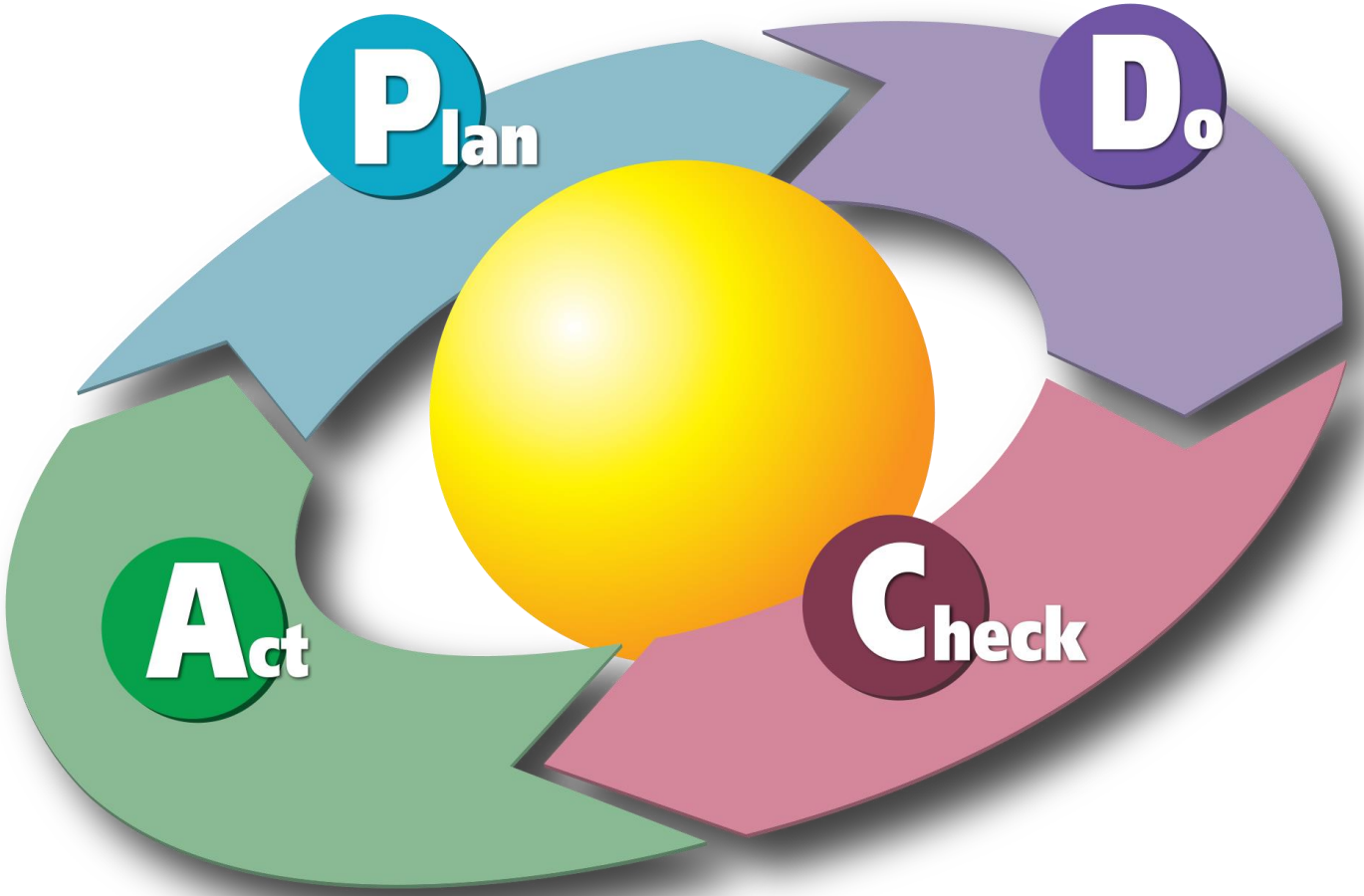
Keys to Success

It's all about Building Trust

1. Build Awareness
    a) Focus on the facts.
    b) Use industry data: There are several reputable sources that show the importance of security in the SDLC. The sources can be found in the best practice side of things as well as incident response.
2. Get Executive Buy-In
    a) Discuss Reputation
        i. Evangelize about protecting the brand/public perception.
        ii. Require executives to establish the organization's reputation's worth.
        iii. Educate executives on the impacts to reputation in the event of a compromise.
    b) Protect sensitive data (PII, CC data, intellectual property and proprietary information).
3. Be Consistent.



Cycle/Repeat




RISK
SECURITY

Appendix:
ISMS Required Actions Details

Information Security Management Required Actions:

Implement and Operate

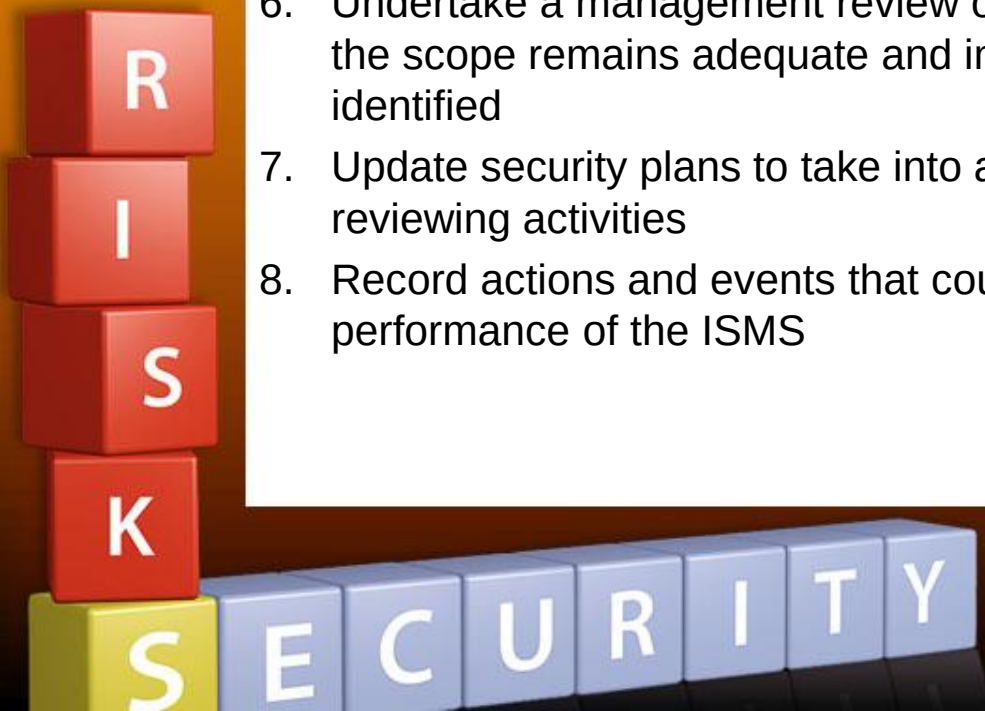
1. Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks
2. Implement the risk treatment plan in order to achieve the identified control objectives
3. Implement controls selected to meet control objectives
4. Define how to measure the effectiveness of the selected controls or groups of controls..
5. Implement training and awareness programs
6. Manage operation of the ISMS.
7. Manage resources for the ISMS
8. Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents

Source: ISO 27001 Information security management systems requirements

Information Security Management Required Actions Continued:

Monitor and Review

1. Execute monitoring and reviewing procedures
2. Undertake regular reviews of the effectiveness of the ISMS
3. Measure the effectiveness of controls to verify that security requirements have been met.
4. Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks, taking into account changes
5. Conduct internal ISMS audits at planned intervals
6. Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified
7. Update security plans to take into account the findings of monitoring and reviewing activities
8. Record actions and events that could have an impact on the effectiveness or performance of the ISMS



Source: ISO 27001 Information security management systems requirements

Information Security Management Required Actions Continued:

Maintain and Improve

1. Implement the identified improvements in the ISMS.
2. Take appropriate corrective and preventive actions in accordance applying the lessons learned from the security experiences of other organizations and those of the organization itself
3. Communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.
4. Ensure that the improvements achieve their intended objectives

Source: ISO 27001 Information security management systems requirements