Technology Risk Management and Information Security
A Practical Workshop

Paul Doelger
Chief Risk Officer - Technology and Business Partners
BNY Mellon
Email: paul.doelger@bnymellon.com

Oct 1, 2010

Agenda

1	Technology and Information Security (IS) Risk Management
2	How to Develop and/or Enhance an Information Security Program
3	Information Security (IS) Testing
4	Computer Security Incident Management
5	Conclusion

Technology and Information Security (IS) Risk Management

Note – The Information Security (IS), risk management, assessment, and mitigation terminology and framework used in this presentation were obtained using the National Institute of Standards & Technology (NIST) Methodology

Information Technology (IT) and Information Security (IS) Risk Management*

IT and IS risk management each encompass three processes:

- Risk assessment
- Risk mitigation
- Evaluation and assessment

The key personnel who should support and participate in these risk management processes include:

- Senior Management
- Chief Information Officer (CIO)
- System and Information Owners
- Business and Functional Managers
- Information Security Officer(s)
- IT Practitioners (infrastructure and application development personnel)
- Business Users

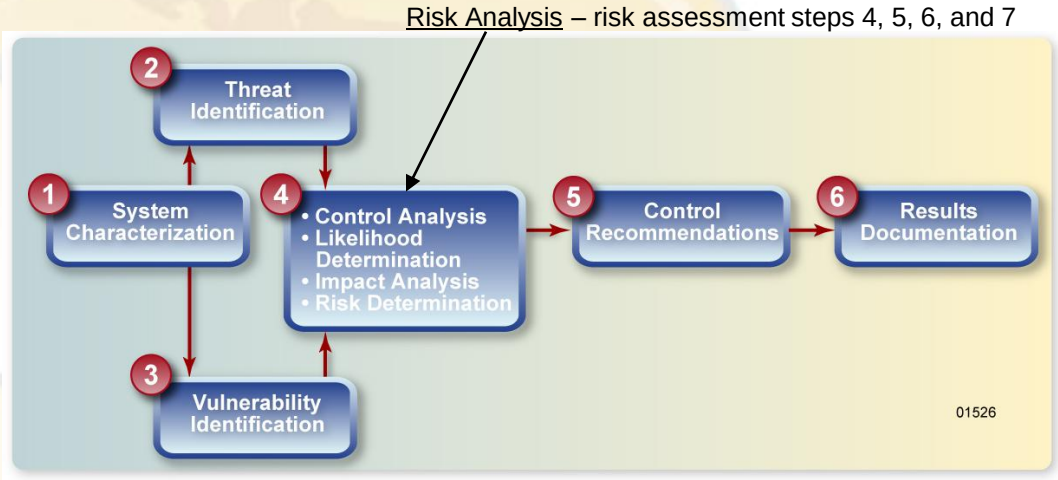
* Note – The risk management, assessment, and mitigation terminology and framework used in this presentation were obtained using the National Institute of Standards & Technology (NIST) Methodology

IT and IS Risk Assessment*

Risk is a function of the ***likelihood*** of a given ***threat*** exercising a particular potential ***vulnerability***, and the resulting ***impact*** of that adverse event on the organization.

The risk assessment methodology encompasses nine primary steps:

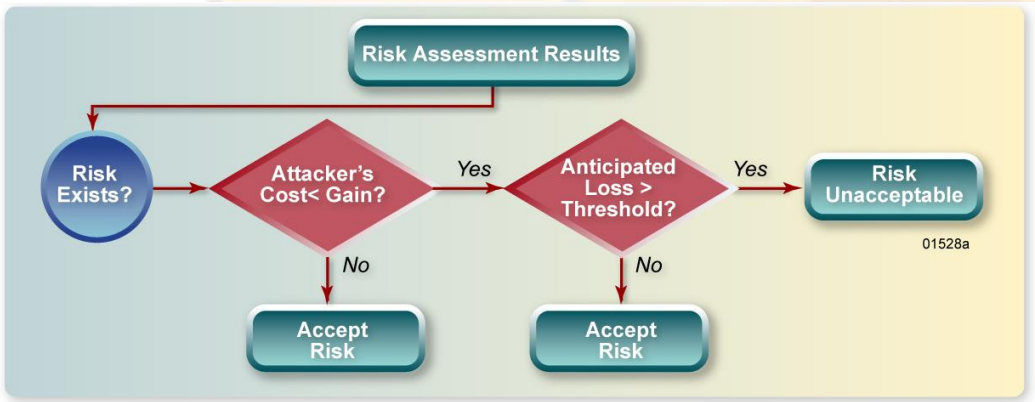
- 1- System Characterization
- 2 -Threat Identification
- 3 - Vulnerability Identification
- 4 - Control Analysis
- 5 - Likelihood Determination
- 6 - Impact Analysis
- 7 - Risk Determination
- 8 - Control Recommendations
- 9 - Results Documentation



* Note – The risk management, assessment, and mitigation terminology and framework used in this presentation were obtained using the National Institute of Standards & Technology (NIST) Methodology

IT and IS Risk Mitigation*

IT and IS risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment.



If you deem the risk to be unacceptable:

1. Prioritize your actions
2. Evaluate recommended control options
3. Conduct cost-benefit analyses
4. Select controls
5. Assign responsibility
6. Develop an implementation plan
7. Implement selected control(s)

*Note – The risk management, assessment, and mitigation terminology and framework used in this presentation were obtained using the National Institute of Standards & Technology (NIST) Methodology

Risk Mitigation Options

- IT and IS risk mitigation can be achieved using any one or combination of the following risk mitigation options:
  - **Risk Assumption -** Accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
  - **Risk Avoidance -** Avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
  - **Risk Limitation -** Limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)
  - **Risk Planning -** Manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
  - **Research and Acknowledgment -** Lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
  - **Risk Transference -** Transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Evaluation and Assessment

- Evaluate and document all outcomes of the IT and IS risk assessment and mitigation processes
  - Create a technology risk management plan
  - Create an information security plan
  - Create an incident response plan
- There should be a specific schedule for assessing and mitigating enterprise IT and IS risks
  - The risk assessment process should be performed using a sliding risk scale
    - High Risk – at least annually
    - Medium Risk – every other year
    - All others – every 3 years

    } Tailor depending on organization priorities
  - The risk assessment process should also be conducted if there is a material change to your IT system, threat vectors, or regulatory requirements (e.g. new applications, cyber criminals, mergers, acquisitions, organic growth, etc.)
  - The risk mitigation process should be performed based on the risk impact identified during the assessment and mitigation activities

How to Develop and/or Enhance an Information Security (IS) Program

Note – The Information Security (IS), risk management, assessment, and mitigation terminology and framework used in this presentation were obtained using the National Institute of Standards & Technology (NIST) Methodology

Information Security Drivers

Client requirements

- Implement and maintain best in class Information Security and Data Protection programs.
- Deliver industry leading data security solutions as a competitive advantage to clients and prospective clients.

Regulatory requirements

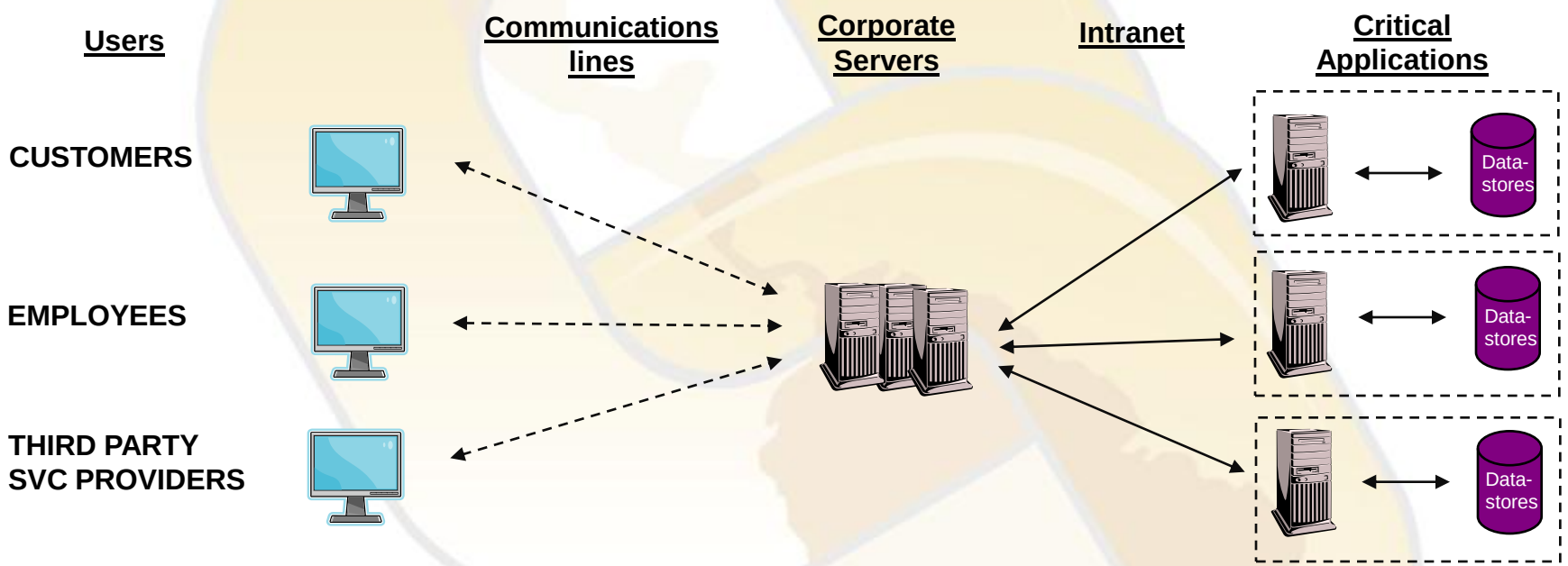
- Manage regulatory and legal impacts proactively and effectively
- The following laws and regulations define requirements for the legal and regulatory landscape regarding information security and the protection of customer information:
  - The Gramm-Leach-Bliley Act (“GLBA”) / SEC Regulation S-P
  - Federal Financial Institution (FFIEC) Guidelines
  - ISO27001 (ISO/IEC 27001:2005)
    - The international standard for Information Security Management Systems
  - International Data Protection Laws – (e.g. EU Data Directive)
  - BS10012 (Personal Information Management System)
  - Numerous US State ID Theft Laws
  - Numerous US State Data Breach and SSN Laws
  - State Information Security Laws (i.e., Massachusetts 201 CMR 17.00)

Business & technology requirements

- Empower business partners to operate securely while meeting customer needs
- Manage a broader set of information risks that will enable the enterprise to meet or exceed sales and operational goals
- Become proactive in the management of information security risks
- Mitigate threats that are increasing in sophistication and number
- Minimize infrastructure, product, and process vulnerabilities

Information Touch Points

What Do We Need To Protect???



THREATS/ VULNERABILITIES	• Cyber Criminals • Third Party Service Providers • Insider Threats • Man in Browser	• Sniffers • Man in the Middle • Theft and fraud • Denial of service • Social Media	• Hackers • Malware • Employees • Config Mgmt • Theft and fraud • Vandalism	• Data alteration • Data Theft • Company Proprietary Information • Employee Error • Config Mgmt Systems	• Unsecured Systems • Compromised Infrastructure • Employees • HW/SW failure

Note – Controls should be established for all known threats and vulnerabilities. This is a reason why the risk assessment activity is so important.

Information Security Threats – Yesterday and Today

2000*

- Default installs of operating systems and applications
- Accounts with No Passwords or Weak Passwords
- Non-existent or Incomplete Backups
- Large number of open ports
- Not filtering packets for correct incoming and outgoing addresses
- Non-existent or incomplete logging
- Vulnerable Common Gateway Interface (CGI) Programs

2010*

- Malware
- Malicious insiders
- Exploited vulnerabilities
- Mobile Devices
- Cyber espionage
- Social networking
- Social Media Attacks
- Zero-day exploits
- Cloud computing

* - SANS Institute - The Top 10 Most Critical Internet Security Threats (2000) and net-security.org Top 10 information security threats for 2010

Information Security Vulnerabilities

Make sure to address both application and infrastructure vulnerabilities

- Unsecured/Unmonitored Remote Access
- Memory safety violations (buffer overflows)
- SQL injection
- Code injection
- E-mail injection
- Accounts with Excessive Privileges
- Misconfigured Routers
- Unpatched, Outdated, and “Default” Software
- Missing or Inadequately Documented Policies, Standards,& Procedures
- Excessive File & Directory Privileges

Development of an Information Security (IS) Program

1- Initiation

- Form an IS Steering Committee
- Conduct a project kick-off meeting
- Determine IS responsibilities
- Confirm goals, scope, and priorities
- Select a framework for the IS program
- Define & document system boundaries
- Begin creation of a IS project plan

2 - Assessment

- Conduct an IS risk assessment
- Identify system boundaries
- Identify your threats
- Identify your vulnerabilities
- Identify and analyze existing controls
- Identify your critical control gaps
- Create Threat Model

3 - Solution

- Use threats, vulnerabilities, and control gaps to identify risks
- Determine likelihood of occurrence
- Quantify risk impact
- Develop plans to remediate risks
- Determine your risks and begin risk mitigation efforts

4 - Implementation

- Implement control recommendations
- Enhance application development and infrastructure controls
- Create an Information Security training program – begin delivery to the organization
- Update the IS plan as needed

5 - Operations

- Test and validate application development and infrastructure controls
- Execute policies and procedures
- Continue delivery of training materials
- Execute your IS communication plan
- Gather stakeholders for final approval

6 – Continuous Evaluation

- Continually update the Plan/Program
- Continue to test and verify controls
- Implement improvement opportunities/recommendations
- Update your program as needed – Revisit phases 1 -> 5 as necessary
- Document results

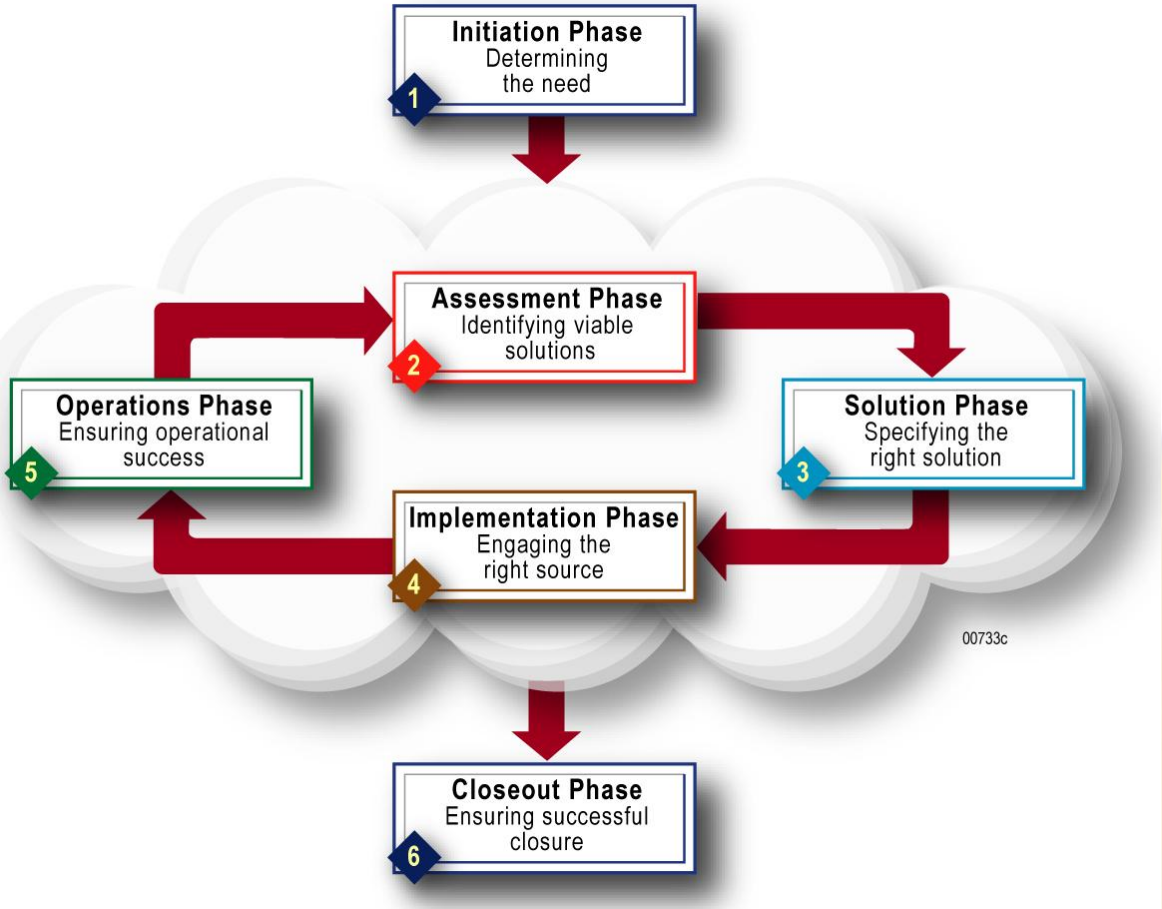
IS Plan Content

Using the threats, vulnerabilities, controls and risks identified in the IS risk assessment, create an IS plan to address:

- IS risk assessment results
- Threats and Vulnerabilities
- Security policies and procedures
- Regulations and laws
- Configuration management and control
- Business Continuity and Disaster Recovery
- Incident response planning
- Security training
- Physical / Logical security
- Personnel security
- Security assessments
- Access control mechanisms
- Identification & authentication mechanisms
- Encryption mechanisms
- Boundary and network protection devices
- Intrusion Protection and Detection systems
- Security configuration settings
- Anti-virus, anti-spyware, anti-spam protection
- Testing and auditing

Many plan templates are available on the net

Information Security Project Life Cycle



- With minor changes, IS project phase names are the same as the IS program phase names on the previous slide
- The major difference is that the activities within each phase are tailored (Program versus Project)
  - The IS program does not closeout. It should be continually evaluated and improved where necessary

Information Security (IS) Testing*

Note – The Information Security (IS) Test assessment framework used in this presentation was obtained using the National Institute of Standards & Technology (NIST) Methodology

Information Security (IS) Testing

- Many test and examination techniques can be used to assess the security posture of systems and networks.
- IS testing should also use a layered approach in order to maximize the effectiveness of your IS test program. You should consider a combination of the following techniques in the creation of your IS test program:
  - Review Techniques
    - These are examination techniques used to evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities, and are generally conducted manually.
    - They include reviews of documentation, logs, rule sets, system configuration, network sniffing; and file integrity.
  - Target Identification and Analysis Techniques.
    - These testing techniques are used to identify systems, ports, services, and potential vulnerabilities. They may be performed manually but are generally performed using automated tools.
    - They include network discovery, network port and service identification, vulnerability scanning, wireless scanning, and application security examination.
  - Target Vulnerability Validation Techniques.
    - These testing techniques corroborate the existence of vulnerabilities and may be performed manually or by using automatic tools
    - Target vulnerability validation techniques include password cracking, penetration testing, social engineering, and application security testing.
  - Third Party Service Provider Validation
    - These testers can provide expertise that is not always found in your internal IS group
    - These testers will generally use a combination of the above techniques to evaluate the quality of your security controls
    - These testers will provide you with an independent, third party opinion

* Note – The risk management, assessment, and mitigation terminology and framework used in this presentation were obtained using the National Institute of Standards & Technology (NIST) Methodology

Organization Considerations - IS Testing

- Organizations should carefully consider risk when selecting testing techniques.
- Some techniques, such as penetration testing, could lead to loss of system availability or exposure of sensitive data.
- Organizations should consider whether testing should be performed on production systems or similarly configured non-production systems.
- Options to consider when making your decisions include:
  - The possible impact to the production systems
    - If a particular test technique is likely to cause a denial of service, it should be exercised using a non-production system.
  - The presence of sensitive personally identifiable information (PII)
    - If testing could expose sensitive PII—such as Social Security numbers (SSN) or credit or debit card information to individuals who are not authorized to have access, organizations should consider performing their testing on a non-production system with an **obfuscated version** of the PII (e.g., test data instead of actual PII).
  - How similarly the production and non-production systems can be configured
    - Many times test environments are not configured (from a security perspective) the same as production environments
- Test/Assessor Selection and Skills
  - The results of your tests can only be as good as the skill set of the test team.
  - Properly vetted, skilled, and experienced assessors will lower the risks involved in conducting security tests.
  - Testers/Assessors should have significant security and networking knowledge, including expertise in network security, firewalls, intrusion detection systems, operating systems, programming, and networking protocols.

Computer Security Incident Management

Note – The Computer Security Incident Management framework used in this presentation were obtained using the National Institute of Standards & Technology (NIST) Methodology

Computer Security Incident Life Cycle

A *computer security incident* is a violation (perceived or real) or imminent threat of violation of your firm's computer security policies/procedures or standard security practices.

- **Preparation** - establish and train an incident response team, develop policies and procedures, and acquire the necessary tools and resources
- **Detection and Analysis** - profile network and system operations (includes applications) and understand their normal behavior. Implement tools/systems to assist in detection and analysis.
- **Containment, Eradication, and Recovery** – identify the potential damage/impact to your organization, the steps required to eliminate/mitigate the executed threat, and the short and long term steps needed to remediate
- **Post Incident Activity** - learn and improve. Enhance your incident response plan, policies, and procedures to better reflect new threats, improved technology, and lessons learned

Note – The incident and risk management, assessment, and mitigation terminology and framework used in this presentation were obtained using the National Institute of Standards & Technology (NIST) Methodology

Incident Response Plan

The first thing to start with is the creation of an incident response plan. At a minimum, the plan should contain:

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with all required parties
- Incident Handling Procedures
- Metrics for measuring the incident response capability
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization.

Incident Handling Procedures

Many pieces of information must be collected, organized, and analyzed to enable the right decisions to be made and executed. Your incident handling procedures should include sections that address:

- Procedures for establishing, documenting, maintaining, and exercising on-hours and off-hours contact and notification mechanisms for various individuals and groups within the organization
- Planning and documenting guidelines for the prioritization of incident response actions based on business impact
- Preparing one or more individuals to act as lead associates responsible for gathering information from the incident handlers and other parties
- Distributing relevant information to the parties that need it
- Practicing the handling of large-scale incidents through exercises and simulations on a regular basis **(An excellent tool to train and prepare all levels of management in your firm)**
- Key individuals to be contacted and begin remediation efforts

Incident Types

A *computer security incident* is a violation or imminent threat of violation of your firm's computer security policies/procedures or standard security practices. Examples of incident types* include:

- Denial of Service (DoS)—an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- Malicious Code—a virus, worm, Trojan horse, or other code-based malicious entity that infects a host
- Unauthorized Access—a person gains logical or physical access without permission to a network, system, application, data, or other resource
- Inappropriate Usage—a person violates acceptable computing use policies
- Multiple Component—a single incident that encompasses two or more incidents; for example, a malicious code infection leads to unauthorized access to a host, which is then used to gain unauthorized access to additional hosts

*Note - this list is not meant to be all inclusive. It addresses the most common types of incidents. Think about your incident types and see if you can adapt it for your organization.

Incident Types and Symptoms

Symptom \ Incident Type	Denial of Service	Malicious Code	Unauthorized Access	Inappropriate Usage
Access to Critical Files	Low	Medium	High	Low
Inappropriate Content - Files	Low	Medium	Low	High
Host Crashes	Medium	Medium	Medium	Low
Unusual Incoming Port Scans	High	Low	Medium	Low
Unusual Outgoing Port Scans	Low	High	Medium	Low
High Bandwidth Utilization	High	Medium	Low	Medium
High Email Utilization	Medium	High	Medium	Low

Incident Response Communications

*Note – The incident and risk management, assessment, and mitigation terminology and framework used in this presentation were obtained using the National Institute of Standards & Technology (NIST) Methodology

Incident Management Recommendations

- Establish strategies and procedures for analyzing, detecting, and containing incidents – INCIDENT MANAGEMENT IS A PROCESS AND NOT A REACTION!!!
- Establish guidelines for the conduct of table top exercises – PRACTICE MAKES PERFECT!!!
- Acquire tools and resources that may be of value during incident handling
- Follow established procedures for evidence gathering and handling – DO NOT TAKE SHORT CUTS. THIS CAN NOT BE OVERSTATED!!!
- Prioritize incidents by business impact, based on the criticality of the affected resources and the technical effect of the incident – ALWAYS RESPOND TO THE HIGHEST PRIORITY INCIDENTS FIRST!!!
- Obtain system snapshots through full forensic disk images, not file system backups – PARTICULARLY IMPORTANT IF YOU ARE ATTEMPTING TO PROSECUTE CRIMINALS!!!
- Capture volatile data from systems as evidence – PARTICULARLY IMPORTANT IF YOU ARE ATTEMPTING TO PROSECUTE CRIMINALS!!!
- Require a baseline level of system event logging and auditing on all systems – BE PROACTIVE BEFORE THE INCIDENT OCCURS!!!

Incident Management Recommendations (cont'd)

- Create a diagnosis matrix for less experienced staff (similar to Incident Types and Symptoms slide) – EXCELLENT FOR BUILDING INCIDENT MANAGEMENT INTO YOUR CULTURE!!!
- Start recording information as soon as your team suspects that an incident has occurred – SAFEGUARD ALL INCIDENT DATA!!!
- Use centralized logging and create a log retention policy – MAKE SURE YOU REVIEW THE LOGS!!!
- Profile networks and systems - Understand both normal and abnormal behaviors of networks, systems, and applications. USE THIS DATA TO PREPARE FOR AND MANAGE YOUR INCIDENTS!!!
- Develop processes to perform event correlation - PARTICULARLY IMPORTANT IN MULTI COMPONENT INCIDENTS!!!
- Keep all host clocks synchronized – PARTICULARLY IMPORTANT IF YOU ARE ATTEMPTING TO PROSECUTE CRIMINALS!!!
- Perform root cause analysis and hold lessons learned meetings after major incidents – KEY TO PROACTIVE MITIGATION OF FUTURE INCIDENTS!!!
- Help to prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secure – BE PROACTIVE RATHER THAN REACTIVE!!!

Conclusion - Thank You

Questions? →

Paul Doelger
Chief Risk Officer - Technology and Business Partners
BNY Mellon
Email: paul.doelger@bnymellon.com