# *Is Your IT Environment Secure?*

*November 18, 2015*

Sarah Ackerman, Greg Bernard, Brian Matteson

**Clark Schaefer Consulting**

clark schaefer consulting

# *Clark Schaefer Consulting*


- Serving elite and emerging companies with practical solutions
- Specializing in project work that is centered around three core competencies:
  - Risk/Control (e.g., Risk Assessment, Internal and IT Audit, Compliance)
  - Technology (e.g., IT Security, System Changes, Disaster Recovery)
  - Accounting & Finance

# *Introductions*

## Sarah Ackerman, CISSP, CISA

Technology practice leader

- Responsible for overall engagement quality and oversight of security and IT audit projects
- Extensive experience in information security, risk management, IT audit, and other risk/control, IT, and compliance services

# *Introductions*

## Greg Bernard, CISSP, CISA

Manager

- IT/internal audit/security projects
- Experienced in IT and IT security, including security assessments, IT audits, vulnerability management and risk management

## Brian Matteson

Senior Consultant

- Subject matter expert in programmatic IT security review, enterprise risk assessment, insider threat, and APTs

# *Overview*

CIA Triad – Confidentiality, Integrity, Availability:
The three most important components of security

**Participants will learn:**

- Definition of each element
- How each element affects your business
- Importance of security awareness for the safety of data
- Consequences of ignoring the importance of the CIA triad components
- Methods used to ensure confidentiality
- How to ensure that your information is trustworthy and accurate
- How to guarantee the reliable access to information

# *CIA – Defined*

- Confidentiality – Taking action to ensure there is no unauthorized access to data
  - Confidentiality protects access to data
  - Privacy protects access to a person


- Integrity – Safeguarding data from unsolicited modification or deletion

**INTEGRITY**

- Availability – Ensuring data is available when it is required

# *CIA Triad*

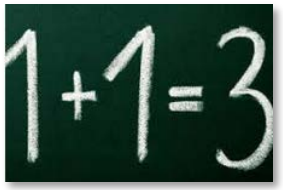
# *CIA – Risks and Controls*

| CIA | Risks | Controls |
|---|---|---|
| **Confidentiality** | • Loss of sensitive data<br>• Unauthorized access | • Access administration and security<br>• Use of cryptography |
| **Integrity** | • Loss of completeness and accuracy<br>• Potential fraudulent activity | • Change monitoring software<br>• Logging<br>• Quality control |
| **Availability** | • Service interruption<br>• Reputational risk<br>• Opportunity Cost | • System backups<br>• Business continuity and disaster recovery planning<br>• Failover testing |

# *Failure to Consider CIA – Consequences*

- Confidentiality – Data leaks and breaches
  - Could lead to compromise of sensitive proprietary/customer information

- Integrity – Use of unreliable data
  - Could have negative impact on downstream systems and processes




- Availability – Unexpected downtime
  - May lead to poor system performance and/or customer dissatisfaction

# *Confidentiality – What you can do*

- Access Control
  - Define user IDs, passwords, and specific access levels (e.g., role-based access)
    - Principle of least privilege
      - Limit access to the minimum necessary for a user's job responsibility
  - Use multi-factor authentication
    - Something you know – password
    - Something you have – proximity card
    - Something you are – fingerprint/retina scans
  - File/document permissions
    - Secure individual files/documents

# *Confidentiality – What you can do*

- Encryption
  - Encrypt data at rest
    - Hard disk encryption
      - Workstations (desktops and laptops)
      - Storage mechanisms (servers)
  - Encrypt data in motion
    - Secure transmission methods (network and transport layers)
      - Prevents compromise of data in transit
    - Use of secure transport protocols (e.g., HTTPS, TLS)
      - Prevents compromise of data in transit
- Segregation of Duties
  - Prevents users from having excessive access to data which is not relevant to their responsibilities within a business process

# *Confidentiality – What you can do*

- 3rd Party Vendor Oversight
  - Ensure that contracts are written to protect
    - Confidentiality agreements / non-disclosure agreements
    - Security considerations – SSAE16 reports
  - Monitor vendor activities
    - Limit access to only what is necessary to perform job
    - Request reports of activities performed
    - Segregate their access

# *Confidentiality – Real Examples of Loss*




2014

- Target and Home Depot were hacked resulting in loss of customer credit card information
  - Demonstrates loss of confidential information
  - Significant reputational damage

- Sony also hacked, resulting in exposure of:
  - Sensitive information about employees
  - Leaks of Sony Pictures films, and other data
  - Attack resulted in loss of intellectual property/ confidential information

# *Integrity – What you can do*

- Physical Integrity
  - Ensure reliability of physical environment where data is stored
  - For example, the following techniques:
    - Uninterruptible power supply (UPS)
    - Redundant array of independent disks (RAID)

- Logical Integrity
  - General controls to help ensure the reliability of data:
    - Referential integrity
      - Ensures that a value in one database table references an existing value in another table
    - Entity Integrity
      - Ensures that each row of a database table is uniquely identified, so that it can be retrieved separately if necessary

# *Integrity – What you can do*

- Logical Integrity
  - Use file integrity/change monitoring software to monitor data and logs
  - Required to meet payment card industry (PCI) standards
    - Sample extract – “Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files, and configure the software to perform critical file comparisons at least weekly”
  - Examples include:
    - Tripwire
    - CimTrak (by Cimcor)

# *Integrity – Real Examples of Loss*

- Recent examples of loss of integrity due to vulnerabilities:
  - **April 2013**: The Associated Press Twitter account was hacked
    - Resulted in false reports of explosions at the White House.
    - Caused a **$136 Billion** drop in value on the stock market
  - **October 2013**: The Syrian Electronic Army hijacked a link from President Obama's Twitter account
    - Redirected to video of terror incidents
  - **January 2015**: Twitter accounts for the New York Post and United Press International were hacked
    - Resulted in publication of erroneous news stories

# *Availability – What you can do*

- Define what data exists and prioritize its importance
- Understand type of storage/retrieval device or media including both hardware and software
- Define and implement the appropriate network bandwidth between devices and network connections of mediums
- Consider the processing overhead of affected mechanisms

# *Availability – What you can do*

- Implement monitoring of service levels with vendors
- Implement effective means of backup to an offsite/disaster recovery location
  - Data replication
  - Data mirroring
  - Frequent periodic backups (e.g., nightly)
- Define and document an effective Disaster Recovery/Business Resumption Plan
  - Defines how to quickly recover data
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)

# *Availability – Examples of Loss*

- Recent examples of loss of availability resulting in system downtime:
  - **PayPal:** Due to a power outage, PayPal services were unavailable for many customers on October 30, 2015
  - **Neustar UltraDNS:** Due to an internal server issue, Neustar UltraDNS, a web content delivery service, was down on October 15, 2015
    - Resulted in 90 minute outage for popular websites, including Netflix and Expedia
  - **CenturyLink:** Result of a software glitch that affected the 911 network overseen by CenturyLink
    - 911 service was down in six western Pennsylvania counties for two hours on October 6, 2015

# *Security Awareness – Tips for Leadership*

U.S. Department of Homeland Security tips for industry leadership:

1. Implement a layered defense strategy that includes *technical*, *organizational*, and *operational* controls

2. Establish clear policies and procedures for employee use of organization's IT systems/data

# *Security Awareness – Tips for Leadership*

3. Coordinate cyber incident response planning with existing disaster recovery and business continuity plans across organization

4. Implement technical defenses
   - For example, firewalls, intrusion detection systems, and Internet content filtering

5. Update your anti-virus software often

# *Security Awareness – Tips for Leadership*

6. Follow your organization's guidelines and security regulations

7. Regularly download vendor security patches for all of your software

8. Change the manufacturer's default passwords on all of your software

# *Security Awareness – Tips for Leadership*

9. Encrypt data and use two-factor authentication where possible

10. If you use a wireless network, make sure that it is secure

11. Monitor, log, and analyze successful and attempted intrusions to your systems and networks

# *Security Awareness – Tips for Employees*

U.S. Department of Homeland Security tips for industry employees:

1. Read and abide by your company's Internet use policy

2. Make your passwords complex.
   - Combination of numbers, symbols, and letters (uppercase and lowercase)

# *Security Awareness – Tips for Employees*

3. Change your passwords regularly (every 45 to 90 days)

4. Don’t share any of your usernames, passwords, or other computer or website access codes

5. Only open emails or attachments from people you know

# *Security Awareness – Tips for Employees*

6. Never install or connect any personal software or hardware to your organization's network or hardware without permission from your IT department

7. Make electronic and physical backups or copies of all your most important work

8. Report all suspicious or unusual problems with your computer to your IT department

# *Security Awareness – Training*

Training Best Practices:

- Modify training program for different departments and/or locations
- Offer different programs for managers and staff
- Provide training more than once per year
- Deliver security awareness training through several different channels
- Measure the success of your company's training program (next slide)

# *Security Awareness – Metrics and Indicators*

| Metric | Indicator |
|---|---|
| Increase in reports of attempted email/phone scams | Better recognition of suspicious emails/calls |
| Reduction in malware outbreaks | Fewer opened malicious emails |
| Vulnerability scans are scheduled to detect high & critical vulnerabilities | Decrease in time between detection and remediation |
| Increase in number of personnel completing training | Attendance tracking and performance evaluations |
| Increase in comprehension of training material | Feedback from personnel; and training assessments |

Source: PCI Security Standards Council

# *Questions?*

# *For More Information*

If you wish to discuss any aspects of this presentation in more detail, please feel free to contact us:

**Clark Schaefer Consulting, LLC.**
120 East Fourth Street, Suite 1100
Cincinnati, Ohio 45202
513-768-7100
www.clarkschaefer.com

Email: info@clarkschaefer.com