Information Technology Risk

Paul Kanneman

National Business Advisory Practice Leader

Grant Thornton

Stephen Landry

Chief Information Officer

Seton Hall University

Agenda

- **Recent developments**
- Seton Hall University's experience
- Defining risk and internal controls
- Types of IT risk
- How to avoid or reduce IT risk
- Summary and Q&A

In the news… 2014

Princeton student reveals way to access student's personal data — Wired Campus

Ohio State says hackers breached data on 760,000 people — NY Times

Inadvertent internal email leads to KCI Clinical breach — The Breach Blog

Data Breach at University of Maryland Exposes 300K Records — CNET

San Diego State University Warns of Possible Data Breach — Threat Post

Backup tapes stolen from New York area Hospital – 1.7 million records stolen — PHIPrivacy

Accounting firm loses flash drive containing over 4,000 patients' information from a NJ area Hospital — PHIPrivacy.net

Healthcare breach in Puerto Rico could affect more than 400,000 people — Databreaches.net

Laptop containing 24,000 patients' information was stolen from a Philadelphia Hospital — Databreacheds.net

Accidentally sent email could end up costing UBS $10 million — Accelion

In the news… 2015

FBI: North Korea behind SONY hack — LA Times

Target says data breach cost $162M — Tech Crunch

Government OPM data breach affected 21M employee records — CNN

Auburn University exposed personal data of 375 students — AL.com

Huge data breach at Anthem — LA Times

100,000 tax returns stolen from IRS Web site — Associated Press

Cyber attacks hit Rutgers, FDU — NJ.com

Penn State College of Engineering hacked in sophisticated cyberattack — Inside Higher Education

Hackers hit University of Virginia — The Hill

UConn reports data breach by Chinese hackers — Inside Higher Education

In the news …

“There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese.”

- James Comey, Director, FBI

(CBS’s 60 Minutes)

In the news …

"Our College of Engineering will emerge from this unprecedented attack with a stouter security posture, and faculty, staff and students in the college will need to learn to work under new and stricter computer security protocols."

- Eric J. Barron, President
Pennsylvania State University

Recent Developments

- Governance landscape
  - Increased accountability for accuracy and integrity in business operations
  - Heightened Board expectations
  - Audit committees' interest in reviewing key controls
  - Concerns about reputational risk
  - Pressures of recent economic downturn

Agenda

- Recent developments
- **Seton Hall University's experience**
- Defining risk and internal controls
- Types of IT risk
- How to avoid or reduce IT risk
- Summary and Q&A

SETON HALL UNIVERSITY

Seton Hall University's IT Risk Journey

- Mid-sized private, Catholic university located in suburban central New Jersey, approximately 15 miles from NYC
- Approximately 6,000 full time undergraduate students, 2,000 full time employees
- Ubiquitous computing campus
- Ranked one of the fifteen "most connected" campuses in U.S. News 2013 survey
- Ellucian Banner / Oracle admin system, fully virtualized data center, moving (slowly) to the cloud (along with everyone else)

Seton Hall University's IT Risk Journey (cont.)

Major Theme:

When it comes to identifying and managing IT Risk, your auditors are your friends!

Seton Hall University's IT Risk Journey (cont.)

- **2005-08:**
  Began implementation of Banner ERP.
  Grant Thornton (GT) was brought in as implementation project manager.
  GT undertook systematic review / reporting of implementation risks.
- **2009-12**
  Expanded risk assessment to include IT-related risks self-identified by IT department.
  Maintained a formal IT Risk Registry.
- **2013-2014**
  University launched a formal Enterprise Risk Management Program.
  IT Risk embedded in nascent ERM Program.

Seton Hall University's IT Risk Journey (cont.)

- **July 1, 2015:**

  University IT Services obtained **$700K in new funding for IT security and compliance initiatives**. Initiated eighteen new IT security and compliance projects, including building out a dedicated PCI compliant subnetwork, database and laptop encryption and multi-factor authentication (MFA).

IT Security Initiatives Planned For FY'2015-16

1 – Upgrade Campus Internet Connection

2 – Augment Server Anti-Malware

3 – Implement Dual Factor Authentication

4 – Reduce PII from IT Systems

5 – Limit Windows Admin on PCs

6 – Encrypt PCs (Staff/Admin.)

7 – Complete PCI Self-Assessment

8 – Enhance Server/Firewall Auditing

9 – Enhance Security Awareness Training

10 – Web Site Security Review

11 – Improve Banner Instance Management

12 – Implement Privileged Access Management

13 – Encrypt Banner

14 – Banner Access Auditing

15 – Banner Application Firewall

16 – SSL Everywhere

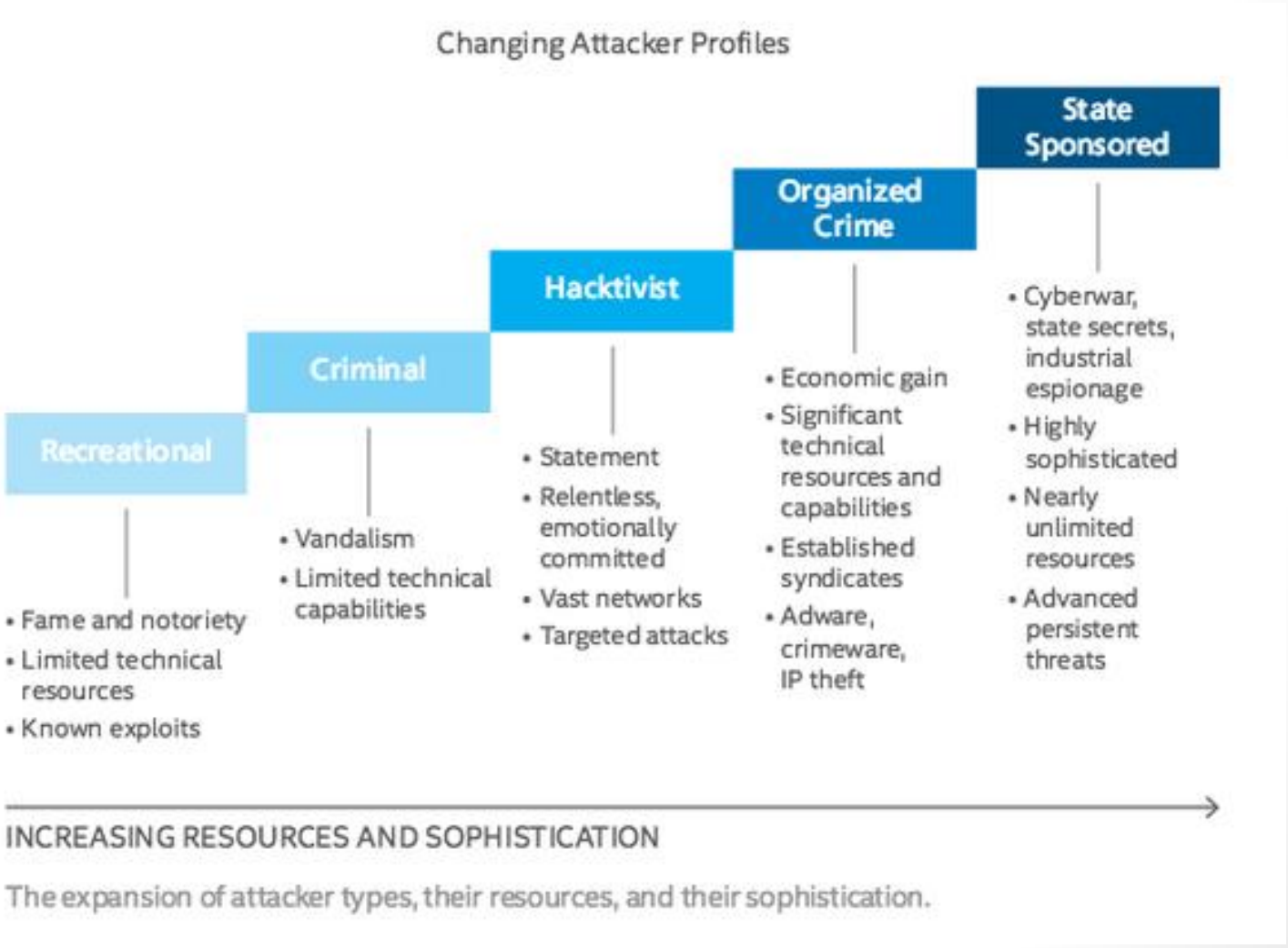
17 – Redesign Banner Job Sub

18 – Improve vendor management practices

Seton Hall University's IT Risk Journey (cont.)

This page intentionally left blank

Seton Hall University's IT Risk Journey (cont.)



Agenda

- Recent developments
- Seton Hall University's experience
- **Defining risk and internal controls**
- Types of IT risk
- How to avoid or reduce IT risk
- Summary and Q&A

Risk Definition

- The **possibility** that a present process or future event will adversely affect the achievement of objectives or negatively impact an asset or some characteristic of value (i.e., **loss**)
- In **information security, "risk"** is defined as a function of four variables:
  - the possibility that there's a **threat** (a declaration of intention to inflict punishment or harm on another)
  - the possibility that there are any **vulnerabilities** (susceptibility to physical or emotional injury or attack)
  - the potential **impact** (magnitude of the potential loss of seriousness of the event)
  - the **likelihood** of an occurrence

Risk Management Definition

Risk management is the process used to **identify**, **source**, and **measure** risk, and the development of **strategies** to manage it

IT Risk Areas
Operational risk

- availability of information
- integrity of information
- adequacy of information
- timeliness of information

} management decision making, business operations and data communication

- constituent/vendor relations; compliance with contractual agreements
- security and privacy; loss of intellectual property

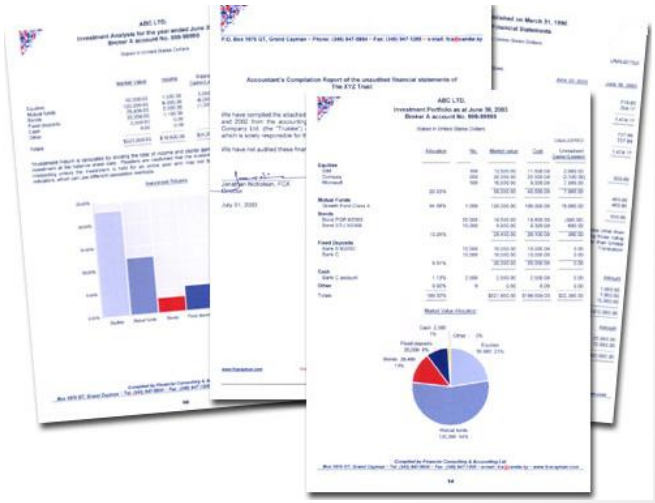
IT Risk Areas
Financial and fraud risk

Financial risk

- accuracy of financial data
- completeness of financial data
- integrity of financial data

Fraud risk

- theft
- misappropriation of assets



IT Risk Areas
Data privacy risk

- As organizations handle ever greater volumes of confidential donor and constituent data**, IT processes and controls must be strengthened to protect such information**
- This data is at **risk of exposure** to external threats
- **Employees who have access to sensitive information** inside an organization also represent a risk
- Greater use of **third-party vendors** and **cloud providers** may introduce additional risks

IT Risk Areas
Compliance risk

Regulatory risk

- HIPAA – Health Insurance Portability & Accountability Act
- HITECH – Health Information Technology for Economic and Clinical Health
- PCI–DSS – Payment Card Industry–Data Security Standards
- Red Flags Rule
- State issued Information Security Breach and Identity Theft Prevention Acts

Accreditation risk

- Institutional accreditation and specialized or programmatic accreditation agencies

Payment Card Industry Data Security Standard (PCI DSS)

Some common PCI myths:

- PCI only applies to retailers and e-commerce sites
- You have to achieve a certain volume of transactions to be subject to PCI-DSS
- PCI compliance means we're secure
- We are PCI compliant if we encrypt cardholder data

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS high-level requirements

The PCI DSS prescribes requirements that any business of any size must adhere to in order to accept payment cards.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a **firewall** configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system **passwords** and other security parameters
Protect Cardholder Data	3. Protect stored data 4. **Encrypt** transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update **anti-virus** software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict **physical access** to cardholder data
Regularly Monitor and Test Networks	10. Track and **monitor** all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a **policy** that addresses information security

Agenda

- Recent developments
- Seton Hall University's experience
- Defining risk and internal controls
- **Types of IT risk**
- How to avoid or reduce IT risk
- Summary and Q&A

Types of IT Risks

- **Data theft / loss** (loss of IP, donor data, id theft, etc.)
  - Employee downloads
  - Improper equipment/media disposal
  - Trojan programs/key loggers/social engineering/phishing
  - Data transmission interception
    - Public hotspots
    - Wireless “leakage”
    - Network “sniffing”
    - Home wireless networks
- **Theft of hardware or services**

Types of IT Risks

- **Loss of data integrity** via manipulation (fraud, malice, error)
- **Intrusion**
  - Physical access to data center/servers
  - Logical access - employees
  - Viruses introduced via remote access connectivity
- **Vendor negligence**
- **Unrecoverable data loss**
- **Reputational risk**
  - Social media
  - Websites visited

Agenda

- Recent developments
- Seton Hall University's experience
- Defining risk and internal controls
- Types of IT risk
- **How to avoid or reduce IT risk**
- Summary and Q&A

Practical Advice in IT Risk Management

- **The Foundation:**
  - **The tone is set at the top** - leadership must support and encourage effective practices to reduce IT risk
  - **Security awareness training** – hackers are targeting your people as much or more than your firewalls and servers

Practical Advice in ITRM (Cont.)

- **The Foundation (Cont.):**
  - **Policies and Procedures**
    - appropriate use of systems
    - who can request and approve access (including vendors)
    - Who can request and approve changes (change control)
    - physical access
    - encryption key management
    - data standards
    - data retention (don’t keep more data than you need)
    - periodic review of access privileges
    - separation of duties
    - reconciliation reports

Practical Advice in ITRM (Cont.)

- **The IT Security Infrastructure:**
  - **Internet Service Provider (ISP)** – first line of defense against "Denial of Service" attacks
  - **Firewall and Intrusion Prevention Systems** (IPS) – your perimeter defense
  - **Network zones** – Do you have defense in depth?
  - **Anti-malware** – protect against phishing
  - **Remote access restrictions** – the more ways for your employees to get in, the more ways for the bad guys to get in, too
  - **System updates, patching & patch management** – eliminate any known vulnerabilities as quickly as possible

Practical Advice in ITRM (Cont.)

- **The IT Security Infrastructure (Cont.):**
  - **Dual Factor Authentication** (a.k.a., Multifactor Authentication or MFA)– A great way to keep the bad guys out.
  - **Firewall and system event logs** – best defense against Advanced Persistent Threats (APS). Do you have a log server / SIEM? Who reviews the logs? How often? How long are logs retained?
  - **Backups / DR Plans** – How often are they tested? How often are backups performed? How are they stored? For how long?

Practical Advice in ITRM (Cont.)

- **The IT Security Infrastructure (Cont.):**
  - Manage (and minimize) your **test and development environments** – they often contain production data
  - **Encryption** – Transmission? Storage? Backups? Everything?
  - **Privileged account management / Data Loss Prevention (DLP)** – Who has access to your most sensitive data? How are they using it? How easy can they give it away, either accidentally or intentionally?
  - **CISO / IT security staffing** – an increasingly important component of ITRM; no security system work alone, someone has to look at it / respond

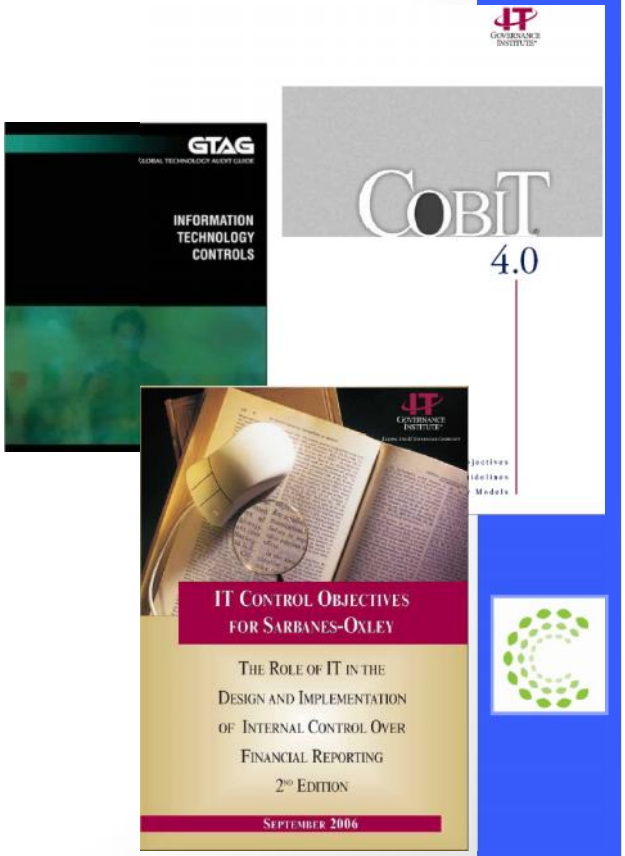
Best Practices in IT Risk Management

- Governance: IT Steering/Advisory Committee
- Business continuity/Disaster Recovery (DR)
- Checklist of legal/regulatory requirements
- System and process controls
- Asset management
- Authoritative data sources / reports
- Eliminate “shadow” systems
- Contracts: require vendor SSAE 16 or right to audit; consider vendor reputation
- Access to network only via “corporate” equipment
- Policy on use of social media by employees
- Regular audits – by IT, Internal Audit, External Auditor
- Security Incident Response Plan

Information Technology Control Resources

The Information Systems Audit and Controls Association (ISACA), the IT Governance Institute (created by ISACA) and the Institute for Internal Auditors (IIA) have all created IT control frameworks and guidelines including:

- Control Objectives for Information and Related Technology (COBIT)
- IT Control Objectives for Sarbanes-Oxley
- Global Technology Audit Guide (GTAG)



ISACA
Serving IT Governance Professionals

IT GOVERNANCE INSTITUTE

The Institute of Internal Auditors

isaca.org
itgi.org
theiia.org

Questions/Comments

Contact information

Paul Kanneman

National Business Advisory Services Practice

Grant Thornton

E: paul.kanneman@us.gt.com

Stephen Landry

Chief information Officer

Seton Hall University

LinkedIn: www.stephenlandry.com

Twitter: @landryst

E: cio@shu.edu