THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

Information Security and Privacy – From a Consulting Perspective

Florida Audit Forum

Semi-Annual Meeting

Tampa, Florida

February 5, 2016

Presenter

Ryan C. Hay, CISA, CISSP, QSA
Manager, Risk Advisory Services
Security and Privacy
West Palm Beach, FL
Ryan.hay@rsmus.com

Agenda

- Incidents and breaches
- Security and privacy 101
- Security and privacy risks in the real world
- Technology to address those risks
- Security and privacy threats and emerging trends
- Recommendations

Incidents and breaches

Recent attacks

TaxSlayer.com

LANDRY'S SEAFOOD

Wendy's

HYATT

Time Warner Cable

THE HOME DEPOT More saving. More doing.

SONY PICTURES

TARGET

U.S. DEPARTMENT OF HOMELAND SECURITY

Chick-fil-A

https://www.privacyrights.org/data-breach

Incident management

- Incident management
  - Ticketing
    - KPI’s
  - Centralized
- Incident response
  - Closure
    - KPI’s
  - Timeliness
- Breach response
  - Notification and communication process
- Forensics

CAUTION
CHAOS FIELD
ESTIMATED STRENGTH: 47 KAZ
LIMIT EXPOSURE TO THIS AREA
AND REPORT ABNORMALITIES
IN YOUR LIFE AFTER EXPOSURE

Incident response

- Not a matter of If, but When?
- Do you have a plan? Plan for failure.
- Make your goal to fail gracefully and minimize damage.
  - Ensure that the business is ready to survive a failure or breach
  - Preventative controls WILL fail at some point
- Communications to those that are impacted
  - Do you know the requirements? Regulatory?
- Testing of the plan
- Post Incident Analysis/Lessons Learned

Security statistics

- Breaches detected in first 24 hours: 1%-2%
- Breaches detected in first month: 35%-46%
- Breaches with data loss in first 24 hours: 60%-68%
- Breaches detected by an external 3rd party: 71%-92%
- Breaches contained within a week: <40%
- Breaches undetected for 2 years or more: >14%
- Average days from breach occurrence to discovery: 87-210

Compiled from:
- Trustwave Global Security Reports
- Verizon Data Breach Investigations Reports
- Symantec Internet Security Threat Reports
- Cisco Annual Security Reports
- McGladrey internal studies
- Multiple other sources

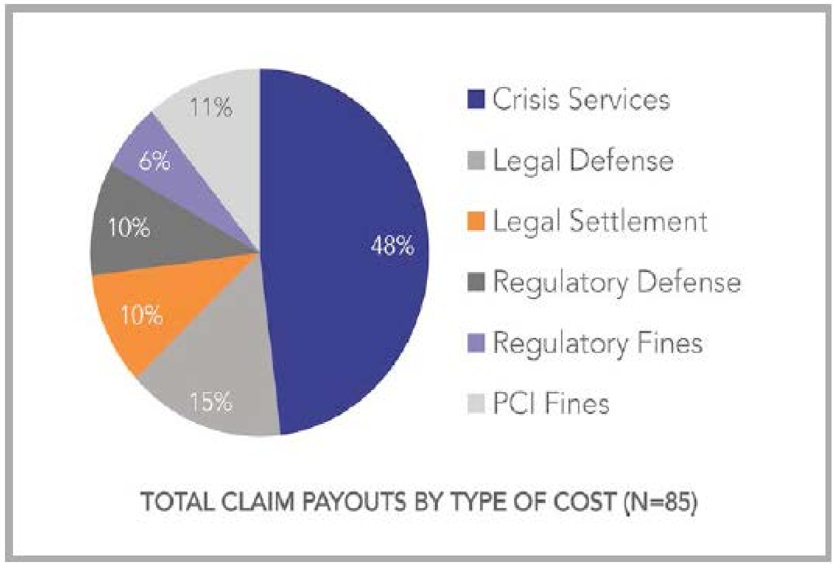
Security Statistics

- Average cost per record of a data breach: $188
- Average records exposed per breach: 28,765
- Average cost spent on notification: $565,020
- Average cost of forensic services: $737,473
- Average cost of post-facto efforts: $1,412,548
  - Combination of costs including hotline, credit monitoring, loss of business, discounts/rebates, fines, etc.
- Average lost business and reputation: $3,030,814
- Average total cost per breach: $5,407,820
- Average insurance payouts: $954,253 - $3.5M

Compiled from:
- 2013 Ponemon Institute Cost of Data Breach: Global Analysis
- NetDiligence 2013 Cyber Liability & Data Breach Insurance Claims
- McGladrey internal studies

Security Statistics

- PII was the most frequently exposed data (41% of breaches), followed by PHI (21%) and PCI (19%)
- Healthcare was the sector most frequently breached (23%), followed closely by Financial Services (22%)
- Small-Revenue ($300M-$2B), Micro-Revenue ($50M-$300M) and Nano-Revenue (< $50M) companies had the most incidents (25%, 24%, 23%)
- Third parties accounted for 20% of the claims submitted
- The average cost for legal defense was $698,797
- The average cost for legal settlement was $558,520

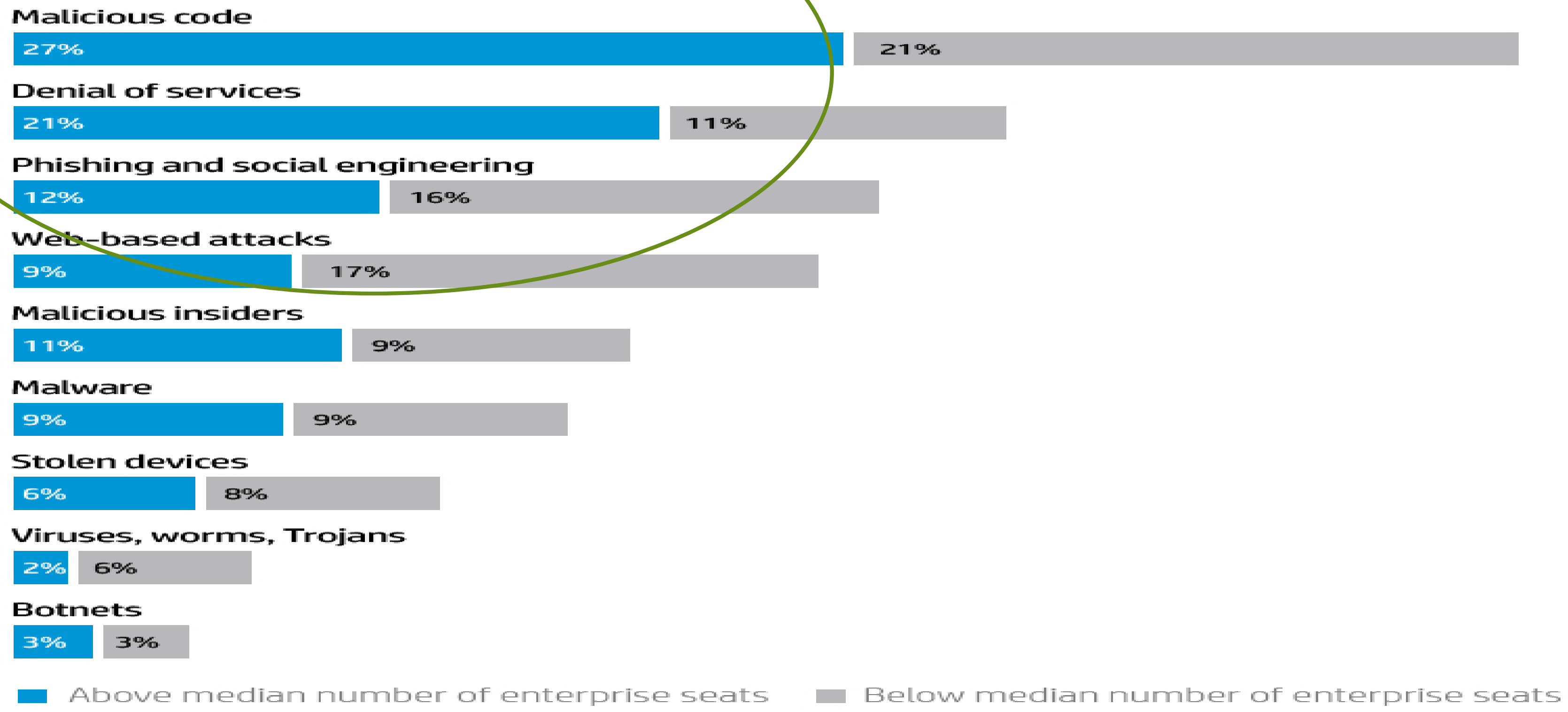


TOTAL CLAIM PAYOUTS BY TYPE OF COST (N=85)

Compiled from:
- NetDiligence/McGladrey Cyber Claims Study

Incident response costs

Percentage of total cost for nine attack types by organizational size



Attacks on smaller and larger organizations are compared based on a sample median of 13,251 seats. Larger organizations experience a higher proportion of costs relating to malicious code, and they have a higher incidence of denial of services.

Source: Ponemon Institute 2015 Cost of Cyber Crime Study

Regulatory compliance

- **Florida Information Protection Act of 2014**

  Signed into law by Florida Governor Rick Scott on June 20, 2014, after it received unanimous support by the legislature. FIPA will take effect on July 1, 2014. Read more: http://www.digitaljournal.com/pr/2008272#ixzz38QUIOmJ3

- 30 day notification (shorter timeline to notify), expanded PII (passport, medical condition, Health policy numbers), Mandatory notice to Florida Attorney General and production of proactive measures (Greater than 500 individuals - written notice of the breach is required to the Florida Department of Legal Affairs, within 30 days (with an additional 15 days upon a showing of good cause). In addition, upon request by the Attorney General, the entity must provide:
  - **A police report, incident report, or computer forensics report;**
  - **A copy of the policies in place regarding breaches; and/or**
  - **Steps that have been taken to rectify the breach.**

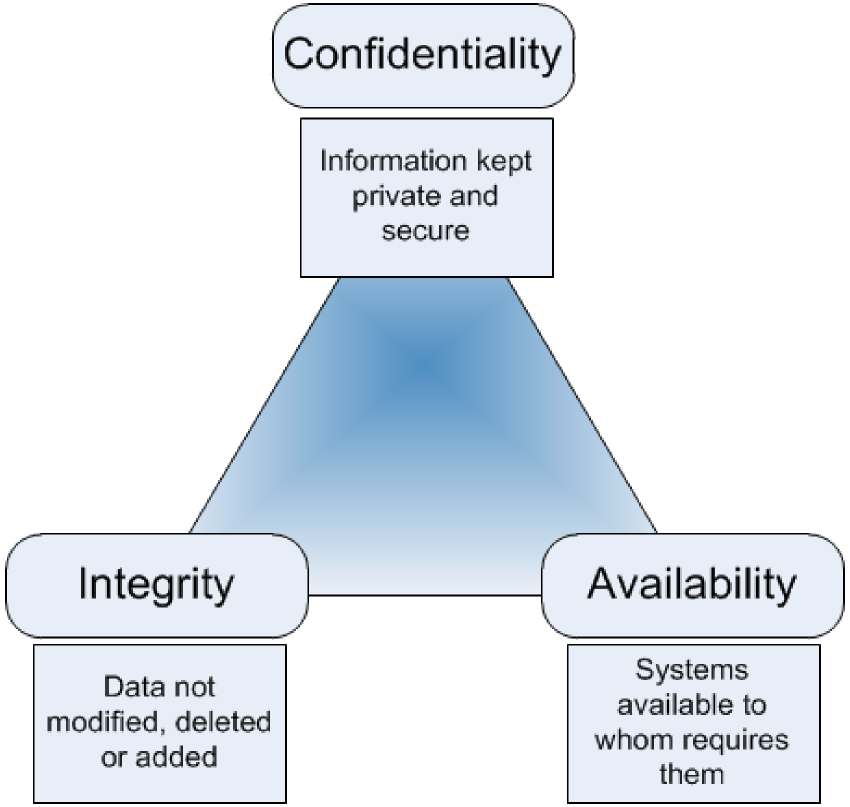
From a consulting perspective

- Attackers are ahead of the technology and controls
- Your controls will fail, governance of processes will fail
- Incident response will continually be tested
- Regulations will continue to place burdens on business
- Process change and reengineering needed to correct
- Continual employment for auditors and consultants

Security and privacy 101

C-I-A Triad

- Principles
  - Confidentiality
  - Integrity
  - Availability
- Safeguards/Controls
  - Administrative, technical, physical
  - Preventative, detective, corrective



Confidentiality

Information kept private and secure

Integrity

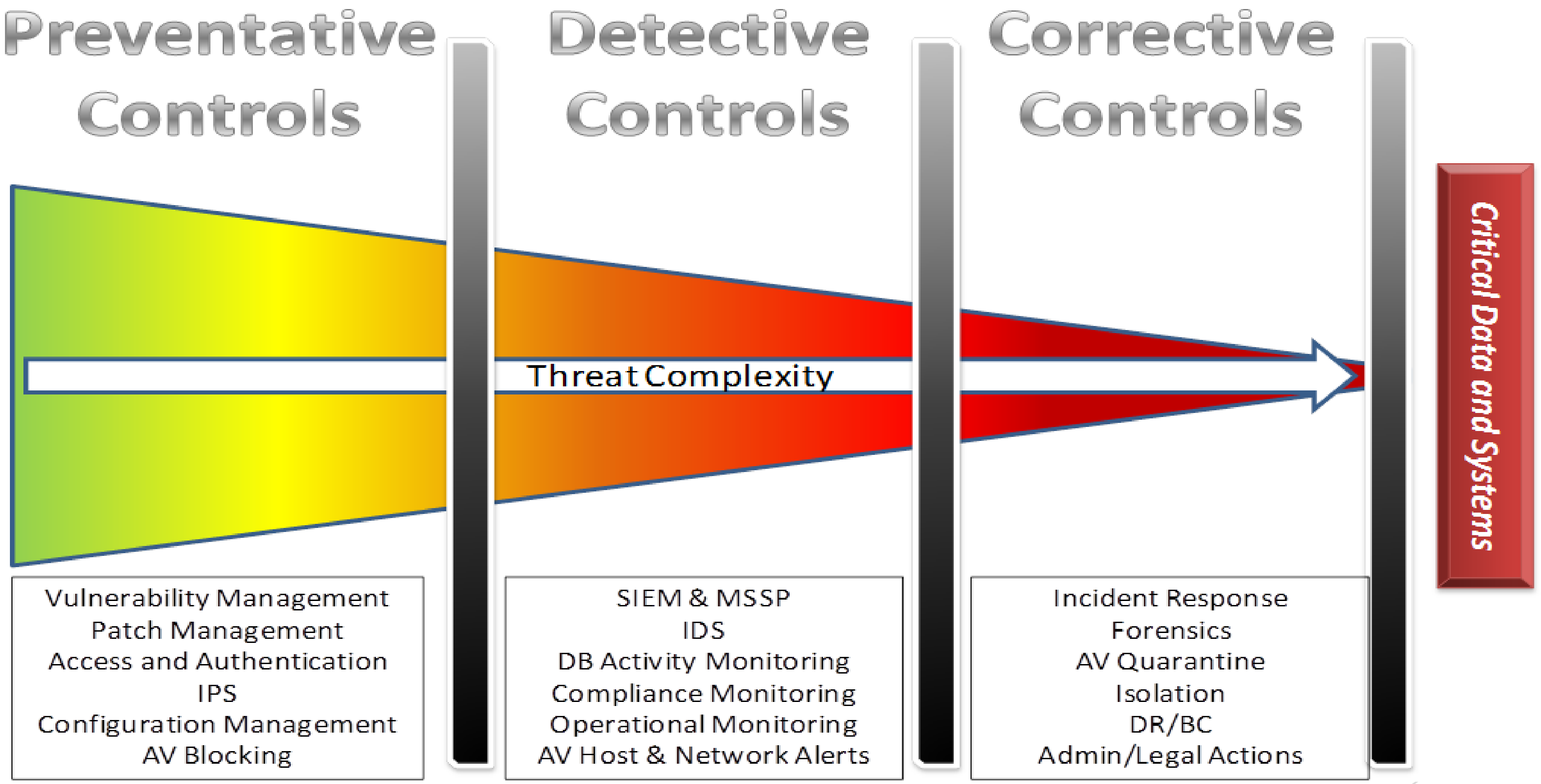
Data not modified, deleted or added

Availability

Systems available to whom requires them

Have you assessed the risk?

Controls to consider



Preventative Controls

Vulnerability Management
Patch Management
Access and Authentication
IPS
Configuration Management
AV Blocking

Detective Controls

SIEM & MSSP
IDS
DB Activity Monitoring
Compliance Monitoring
Operational Monitoring
AV Host & Network Alerts

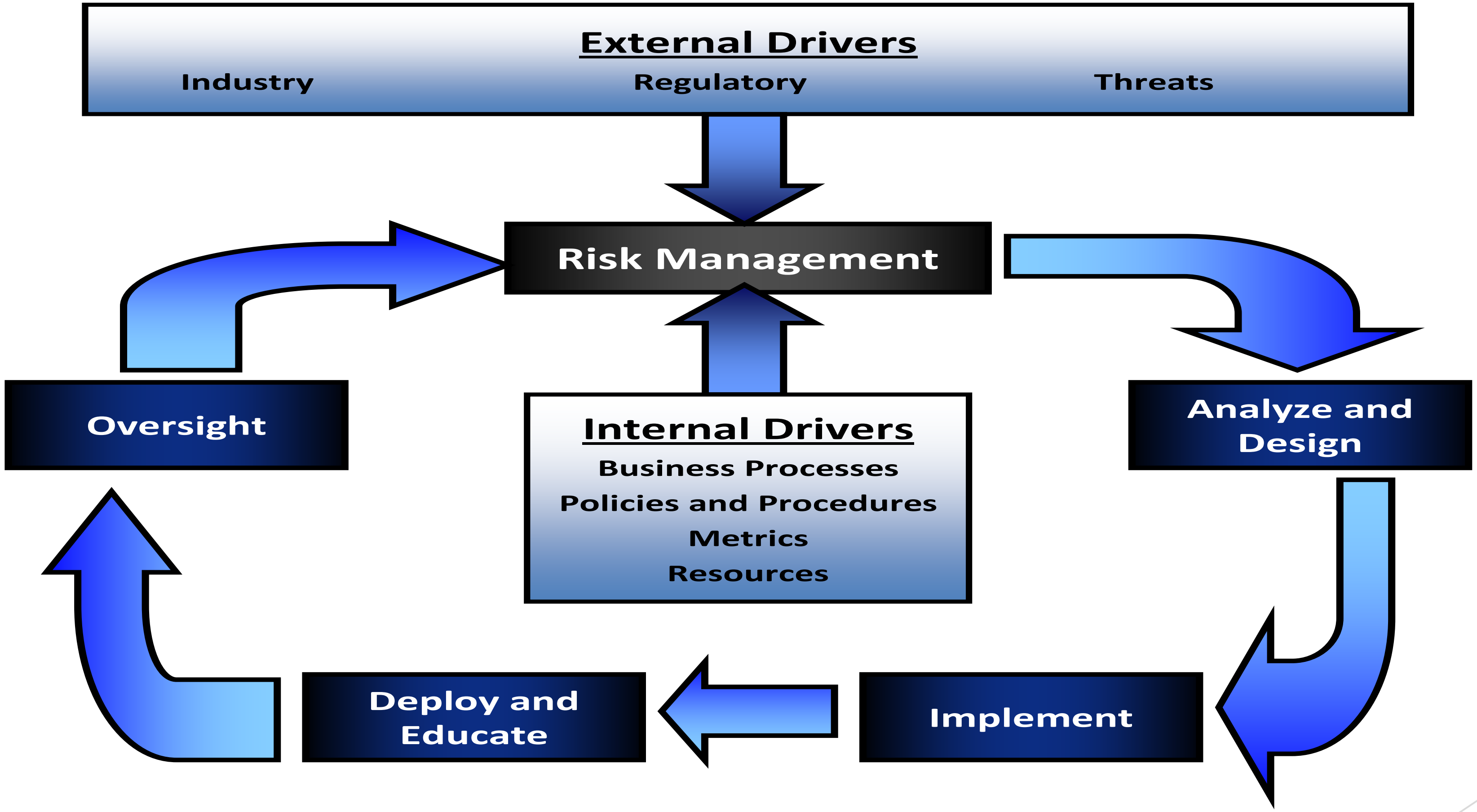
Corrective Controls

Incident Response
Forensics
AV Quarantine
Isolation
DR/BC
Admin/Legal Actions

Threat Complexity

Critical Data and Systems

Risk Assessment



External Drivers

Industry

Regulatory

Threats

Risk Management

Internal Drivers

Business Processes

Policies and Procedures

Metrics

Resources

Analyze and Design

Implement

Deploy and Educate

Oversight

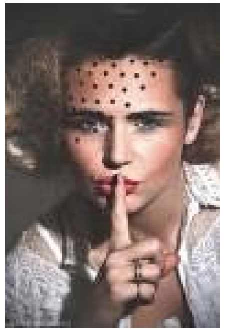
Risk considerations

- Access control (provisioning)
- Change management
- Incident management
- Disaster recovery/business continuity
- Backup/restore/disposal
- Development (SDLC)
- Data governance
- Training and development
- Physical
- Technology/tools
- HR

- Infrastructure/Network
- Logging/monitoring
- Incident response
- Encryption
- Policies and procedures
- Vendor management
- Asset management
- Authentication
- Mobile security
- Data Privacy

Privacy concerns

- What information is collected?
- Why is the information being collected?
- Intended use of the information
- With whom the information will be shared with
- How the information will be secured
- Consent and choice of the data subjects



- Identifiability – How do you identify individuals? SSN
- Quantity of PII - More PII on systems the greater the exposure
- Data Field Sensitivity
  - Departments vary in criticality.
- Context of Use
  - What is the PII used for. Disclosure of PII.
- Obligation to protect PII – HIPAA, GLBA, PCI requires this.
- Access to and Location of PII – access to PII and where located (classification)

Identity verification ???

From a consulting perspective

- Security is not bought
  - Tools are tools, not solutions. You can absolutely do security “on the cheap” if it is done correctly. However, cheaper usually equates to more time and staff
  - Security cannot be successful unless it is embedded in a variety of enterprise policies and processes
- Security threats do not only come from “out there”
  - Attacks by rogue employees, mistakes, and fraud are not common, but result in immense damage when they occur
  - Ensure security plans properly account for these events. Very common that plans only focus on external threats
  - Remember, once the bad guys breach your external boundary they are now a version of insider threat
- Many security threats exist because of failed IT Governance and NOT integrating security into everyday processes

IT Governance

- **Real World Scenarios of failed governance:**

- **2008 Financial Crisis (Lending/Housing)(led to Dodd-Frank)**
- 2000-2 Enron, Lehman Brothers, AIG (Funds mismanagement/Hold execs accountable) (led to Sarbanes-Oxley)
- 1996 Protected Health Information (PHI) (Security and Privacy) (led to HIPAA)
- 2016 - ????

COMMON SENSE
IS LIKE DEODORANT.
THE PEOPLE WHO
NEED IT MOST
NEVER USE IT.

Security Statistics

What are the methods?

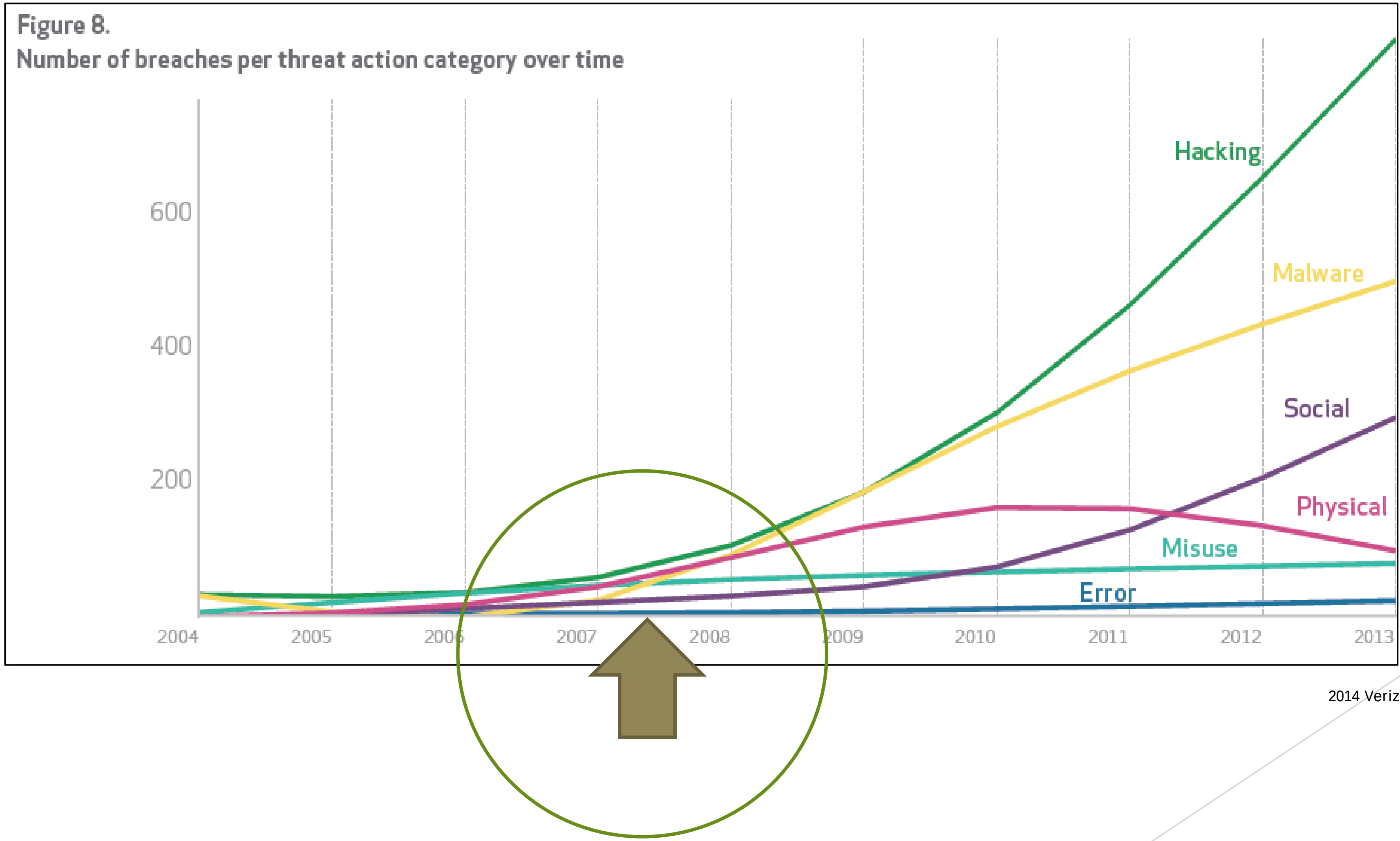


Figure 8.
Number of breaches per threat action category over time

2014 Verizon Data Breach Report

Security and privacy risks in the real world – Audit perspective

Top 5 Risks identified

- 1. Asset Management
- 2. Data governance
- 3. Logging and monitoring
- 4. Incident management and response
- 5. Change management/Development
- 5. Mobile devices (BYOD)

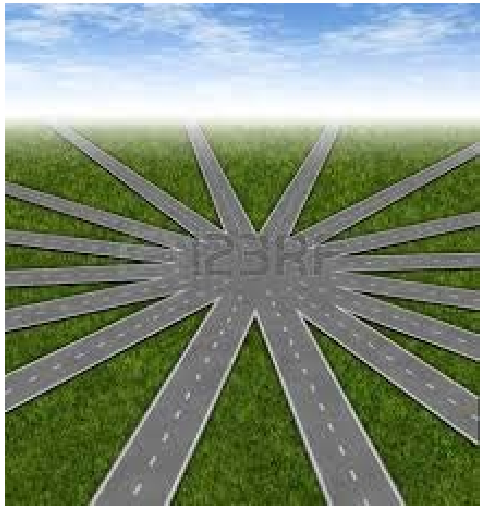
From a consulting perspective

- New risks are exposed daily
- Business struggle with keeping up with risk
- Risk decisions
  - Accept
  - Avoid/Ignore
  - Transfer
  - Mitigate

Technology to address those risks

Technology

- DLP (Data Loss Prevention)
- SIEM (Security Information and Event Management)
- Id/AM (Identity and Access Management)
- IDS/IPS (Intrusion Detection/Prevention System)
- MDM (Mobile Device Management)
- Encryption (PGP, EEE, AES, TLS, SSL)

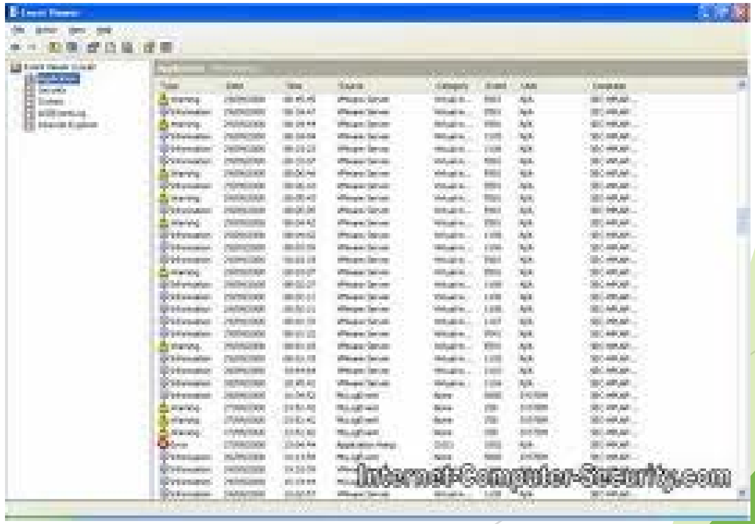


What is DLP?

- **Data Loss Prevention** - is designed to detect and block sensitive data while **in-use** (endpoint actions), **in-motion** (network traffic), and **at-rest** (dat

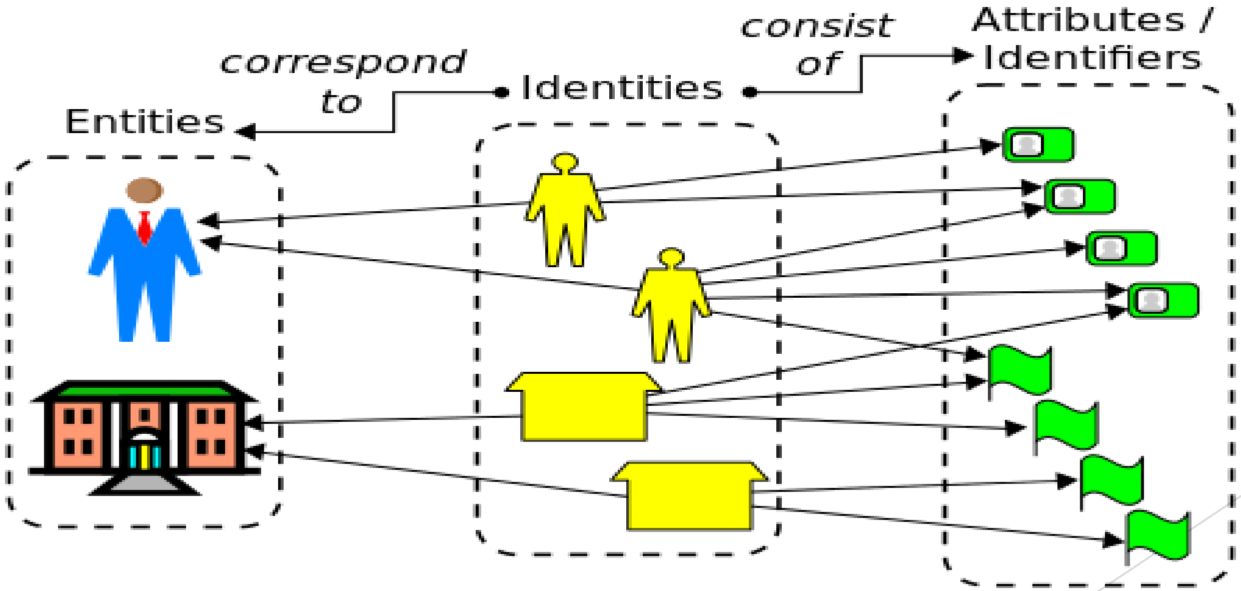
What is SIEM?

- **Security Information & Event Management** - provides real-time analysis of security alerts/logs generated by network hardware and applications. Provides data aggregation, correlation, alerting, and retention capabilities.



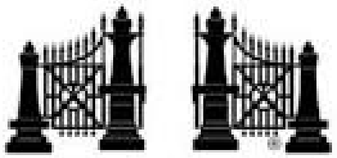
What is Id/aM?

- **Identity & Access Management** – is the management of individual access, authentication, authorization, and privileges within or across system and enterprise boundaries.



What is IDS/IPS?

- **Intrusion detection system** (**IDS**) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.
- **Intrusion prevention systems** (**IPS**) - the main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it



What is MDM?

- **Mobile Device Management (MDM) -** software secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises.

Encryption

- Data at rest, in motion, in-use
  - Whole disk, File level
  - Database, application
  - PGP – contents of message
  - TLS – data in transit
  - SFTP – data in use
  - Certificates (SSL)
  - WPA (Wi-Fi Protected Access), Algorithms
  - Enterprise Email

Security and privacy emerging trends

2016 Breach Trends

- 1. The EMV Chip and PIN liability shift will not stop payment breaches
  - Shift inspired attackers to focus on online transactions where cards do not need to be present
- 2. Big healthcare hacks will make the headlines but small breaches will cause the most damage
  - Healthcare records are worth up to 10x more on the black market than credit cards
- 3. Cyber conflicts between countries will leave consumers and businesses as collateral damage
  - Stealing corporate and government secrets
- 4. 2016 U.S. presidential candidates and campaigns will be attractive hacking targets
  - Nothing new, i.e. Hilary Clinton, Sara Palin email in 2008
- 5. Hacktivism will make a comeback
  - Reputational damage to a company or cause, i.e. Ashley Madison, Twitter Pro-ISIS accounts removed

http://www.securityinfowatch.com/article/12145029/5-data-breach-trends-to-watch-in-2016

From a consulting perspective

1. Mobile devices/Cloud

   - Bring your own cloud (BYOC) is a term being used to define how mobile device users often use a variety of “cloud” services and may accidently or purposely store sensitive information in the “cloud.”

   - The hacking community sees that these cloud service providers are ripe for harvesting sensitive information.

2. Internet of “Things”

   - More and more devices and nontraditional systems are connected to the Internet.
   - Such nontraditional systems are the NEST thermostat, baby monitors, nanny cams, Iris home management systems and others.

From a consulting perspective

3. Wearable computers
   - Google glass, Samsung Galaxy Gear watches and others allow computers (normally with video and audio recording capability enabled) to be used everywhere by anyone.
   - There are many others, such as pens, watches, audio, video, color—even HD!
   - How do you prevent and control their use in sensitive areas?
4. Attacks against unsupported software will increase
   - A LOT of Windows 2000, XP, 2003 is still running in businesses and homes.

From a consulting perspective

- 5. Ransomware
  This is where criminals hijack a user’s ability to access data or systems to extort a payment from victims who hope to have their access restored (FBI virus).

© Original Artist / Search ID: mon776

Rights Available from CartoonStock.com

“This has so many different fonts in it,
I thought it was a ransom note.”

Social engineering

SOCIAL ENGINEERING SPECIALIST

Because there is no patch for human stupidity

- Step 1: Get a target
  - Can be somewhat random (e.g. spam emails) or highly selective

- Step 2: Interact with the target
  - Easier said than done
  - Need to reach them in some way (email, phone, physical, etc.)

- Step 3: Convince them to perform some action
  - Can be as simple as clicking a link or as complex as a full transaction

- Step 4: Leverage the results of the action
  - Simple as direct theft or as complex as full network takeover
  - Major point: Getting an authorized user to perform an action will bypass many standard security controls

Recommendations

From a consulting perspective

- Your incident response plan will be tested
- Controls will fail
- Assessing risk is a daily thing (internal and external)
- Managing risk properly is a daily and continual thing
- Training and awareness balance
- Integrate security into everyday practices
- HR/hiring practices
- Stay current with the latest events
- Embrace the auditor