



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

August 5, 2015



ISOAG August 5, 2015 Agenda

- | | |
|--|--|
| I. Special Announcement & Update | Michael Watson, VITA |
| II. Welcome & Opening Remarks | Michael Watson, VITA |
| III. The Impact of Effective IT Audit Planning | Peter Tsengas & Chadham Hover, Dixon Hughes Goodman LLLP |
| IV. Verizon Data Breach Report | Bhavesh Chauhan, Verizon |
| V. Upcoming Events | Bob Baskette/Michael Watson, VITA |
| VI. Partner/Operation Update | Bob Baskette, VITA, Michael Clark, NG |



Special Announcement and Update

Mike Watson

Commonwealth Chief Information Security Officer



Welcome and Opening Remarks

Michael Watson

August 5, 2015



The Impact of Effective IT Audit Planning

Peter Tsengas & Chadham Hover,
Dixon Hughes Goodman LLP

August 5, 2015

Overcoming the Challenges of Developing and Executing an Effective Audit Plan



Chadam Hover, CISA

Richmond, VA



Senior Consultant, Risk Advisory Services

M 804.282.7636

Chadam.Hover@dhgllp.com

4510 Cox Road, Suite 200 | Glen Allen, VA 23060

Industry Experience

Chadam is a Senior Consultant with seven years of experience in risk advisory, IT Audit, and internal audit.

- Led SOX audits of IS applications and IS control environment of Fortune 500 companies as smaller public companies
- Led audits of IS application and controls environments at large private companies
- Audited IS controls, reports generated from IS applications, automated business processes, segregation of duties controls and organization-wide/entity level controls
- Performed Information System Risk and Control Assessments and recommended control activities to clients for the development of a secure and functional IS control environment
- Performed reviews over IT projects ranging from small updates/upgrades to large scale ERP implementations as well as other more specialized process transformation projects
- Led multiple audits including financial, performance, information technology and security, federal compliance and state government entities
- Member of PeopleSoft implementation team. Dealt extensively with PS General Ledger, Expenses, HRMS, Project Costing modules and security and integration modules

Education

Virginia Polytechnic Institute and State University

- Bachelor of Science, Business

Industry/Service Focus

- IT Project Management
- Information System Security and Assurance
- Financial and Performance Auditing

Licenses & Certifications

- Certified Information Systems Auditor

Professional & Civic Organizations

- Information Systems Audit and Control Association, Member

Peter Tsengas, CISA, CISM

Richmond, VA



Senior Consultant, Risk Advisory Services

M 804.474.1293

Peter.Tsengas@dhgllp.com

4510 Cox Road, Suite 200 | Glen Allen, VA 23060

Industry Experience

Pete is a Senior Consultant with 18 years of experience in risk advisory, IT Audit, and internal audit.

- Performed and led multiple IT Security Audits for various State Government Agencies to assess compliance with Commonwealth of Virginia IT Security Standards (e.g., SEC501-09)
- Assisted with the development of annual IT risk assessments and audit plans
- Performed and led SDLC Audits for major systems development projects at the Virginia Department of Corrections and Virginia Department of Transportation
- Served as the Internal Audit representative on various agency project initiatives, including the DOC IT Transformation Project and DOC Server Migration Project
- Performed and led IT security infrastructure assessments
- Recommended the establishment of an IT Security Governance framework
- Performed and led multiple internal control assessments for business applications
- Recommended enhancements to systems development project requirements, user acceptance testing and training processes
- Assisted management with the implementation of new point of sale systems and oversight of server migration projects
- Recommended the establishment of Board of Directors security awareness reporting methods
- Performed and led reviews of IT vendor management

Education

Virginia Polytechnic Institute
and State University

- Bachelor of Science,
Accounting Information
Systems

Industry/Service Focus

- IT Audit/Internal Audit
- Compliance Audit
- Information Security
Continuity/Disaster
Recovery
- Vendor Management

Licenses & Certifications

- Certified Information
Systems Auditor
- Certified Information
Security Manager

Professional & Civic Organizations

- Information Systems Audit and Control Association, Member

- **Keys to Developing an Effective IT Audit Plan**
 - Communication With Key Members of Management
 - Understanding the IT Environment and its Challenges
 - Awareness of Newly Emerging IT Risks
 - Performing Risk Assessment
 - Other Considerations for the Audit Plan
- **How To Make an Audit Effective “For All Parties”**
 - Potential IT Audit Areas/IT Audit Coverage
 - How the IT Department Can Benefit From an Audit
- **Appendix: IT Audit Coverage/Program**
 - Key Controls
 - Common Audit Findings



Keys to Developing an Effective IT Audit Plan

Communication With Key Members of Management

– Executive Management

- Discuss Goals and Objectives of the Agency Overall
- Mission
- Areas of Concern

– IT Management

- Goals and Objectives of the IT Department
- Understanding the IT Environment (covered further in the following slides)
- New Projects within the IT Department
- Areas of Concern

– Business Unit Management

- Goals and Objectives of the Business Unit
- Planned Changes to Business Information Systems
- Areas of Concern

Understanding the IT Environment



Understanding the IT Environment

Internal Audit should develop an understanding of:

- Anticipated Growth
- Network infrastructure (LAN, WAN, Wireless)
- Use of Advanced Technology
- Number of users
- Amount of change to IT environment
- Application development
- External connectivity (e.g., VPN)
- Web Activity

Understanding the IT Environment

Anticipated growth

- Office locations
- Products and services
- Personnel
- Acquisitions/ mergers = CONVERSIONS

Network infrastructure

- LAN/ WAN/ Wireless
- Internet/ Intranet
- Skill sets of support personnel
- Reliance on vendors

Understanding the IT Environment

Use of Advanced Technology

- Mobile, laptops, wireless, imaging, portals
- Support requirements are elevated
- Skill sets of support personnel

Number of users

- Security administration process
- Personnel needs to support adds/deletes/ changes
- General indicator of specialized IT needs



Understanding the IT Environment

Amount of change to the environment

- Network
- Conversions
- New third party connections

Application development

- In-house vs. third party
- Location of the controls
- Coverage of the controls
- Use of reporting utilities and spreadsheets

Understanding the IT Environment

External Connectivity

- Which third parties get data?
- Security considerations
- Controls at the third parties

Web Activity

- Products and services
- Transactions vs. websites
- Intranet applications and use



Understanding the IT Environment

Challenges that an IT Department can face include.....

- Addressing the growing need for agility
- Breaking free from technical debt
- Balancing data accessibility with security
- Adapting to a connected world (e.g., “The Internet of Things”)
- Bridging the skills gap (e.g., Ability to retain and hire a skilled workforce)
- End-of-Life or Unsupported IT Systems
- Maintaining Compliance with Constantly Changing Regulatory Requirements at the Local, State, and Federal Government Levels

Awareness of Newly Emerging IT Risks

Audit leaders should examine the following risks at their agencies and consider factoring them into current and future audit planning:

- Information Security Breaches
- Data Leakage and Privacy Violations
- Outsourcing Exposure
- Human Resource Risks
- Funding
- Regulatory Concerns

Awareness of Newly Emerging IT Risks

- **Information Security Breaches**
 - Internal data theft
 - Cybercrime - malware, keystroke logging, phishing attacks
 - Identity theft - credit card #s, social security #s, account #s
- **Data Leakage and Privacy Violations**
 - Often unintentional/ caused by carelessness
 - Data leakage from mobile devices/ USB memory devices
- **Outsourcing Exposures**
 - Loss of intellectual property
 - Offsite data storage
 - Same standards/ regulations might not apply to vendor

Awareness of Newly Emerging IT Risks

- **Examples of Information Security Breaches:**
 - Broad New Hacking Attack Detected Global Offensive Snagged Corporate, Personal Data at nearly 2,500 Companies; Operation Is Still Running
 - Hackers in Europe and China successfully broke into computers at nearly 2,500 companies and government agencies over the last 18 months in a coordinated global attack that exposed vast amounts of personal and corporate secrets to theft, according to a computer-security company that discovered the breach.
 - “A global hacking offensive has broken into U.S. companies and government agencies. Cyber attacks could soon be seen as a national security threat”, WSJ executive editor, Jerry Seib, tells the News Hub.

Awareness of Newly Emerging IT Risks

- **Examples of Data Leakage:**
 - **Tax inspector in Vancouver, British Columbia:**
 - Used the Canadian Revenue Agency's computers to look up citizen's tax records for four years
 - Identified high net worth individuals
 - Inspector had a personal business on the side and used information to target prospects

Awareness of Newly Emerging IT Risks

- **Examples of Data Leakage (Continued):**
 - Over a six month period, 12,500 mobile devices were left in taxis
**2009 survey data protection solutions company*
 - 4,500 USB memory sticks were left in pant pockets sent to the dry cleaners
**2009 survey data protection solutions company*
 - Laptops disappearing from security lines at airports



Awareness of Newly Emerging IT Risks

- **Examples of Outsourcing Exposures:**
 - Two of the largest U.S. banks have issued new credit and debit cards to Massachusetts customers after running into data-safety concerns.
 - The banks each recently issued replacement cards to consumers, telling them in the letters that their account numbers may have been compromised.
 - “We have learned that account information from certain debit cards **may have been compromised at an undisclosed third-party location,**” the Bank said in a recent letter to customers in the state. As an added measure of security, the Bank issued a replacement debit card.
 - The bank told credit-card customers in Massachusetts “your account number may have been illegally obtained as a **result of a merchant database compromise** and could be at risk for unauthorized use.”

Source: Charlotte Business Journal

- **Examples of Human Resources Risk:**
 - Network administrator for city of San Francisco
 - Disgruntled about his imminent dismissal
 - Refused to hand over administrative credentials
 - Left the city without control of the network for 12 days
 - \$900,000 to reconfigure routers
 - Felony conviction of denying computer services

Performing Risk Assessment

General approach to assessing risk:

- Identify internal and external threats
- Assess the likelihood and potential damage of the threats
- Assess the sufficiency of policies, procedures, and systems in place to control risk = CONTROLS
- Inherent risk, control risk, and residual risk should all be considered

IT Risk Concepts – Inherent Risks:

Measuring Inherent Risk

Inherent Risk = risk found in the environment and in human activities that is part of existence

Risk Category – People

- Number of resources
- Matching competencies/ skill sets
- Compensation history
- Location constraints
- Training programs
- Turnover history



IT Risk Concepts – Inherent Risks (Continued):

Measuring Inherent Risk

Risk Category – Processes

- Policies and procedures documented
- Maturity level of process
- Manual versus automated
- New product or service
- Distributed versus centralized operations
- Monitoring effectiveness

IT Risk Concepts – Inherent Risks (Continued):

Measuring Inherent Risk

Risk Category – Technology

- Complexity of the environment
- Reliance on third parties
- Stability and reliability of environment

Performing Risk Assessment

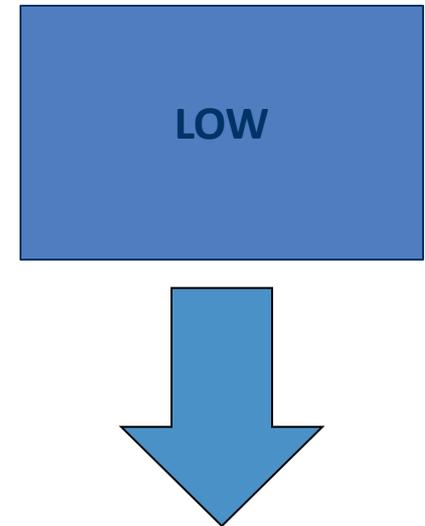
IT Risk Concepts – Control Risk:

Measuring Control Risk

Control Risk = mitigating factor that reduces the likelihood that the aggregate inherent risk will materialize

Low

- Minor issues identified in recent audits
- Management has a sound remediation process in place
- Last internal audit was performed within the previous 12 – 24 months



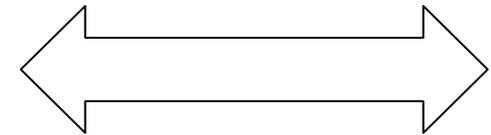
Performing Risk Assessment

IT Risk Concepts – Control Risk (Continued)

Measuring Control Risk

Moderate

- Issues identified in previous audits
- Management's remediation process is adequate
- Last internal audit was performed within the previous 24 – 36 months
- Nature of findings in prior audit required management's commitment to correct



Performing Risk Assessment

IT Risk Concepts – Control Risk (Continued)

Measuring Control Risk

High

- Significant issues still unresolved from previous audits performed
- Management's remediation efforts are not operating effectively
- No internal audits performed in the past 36 months
- Nature of findings in prior audit required management's immediate attention



HIGH

Performing Risk Assessment

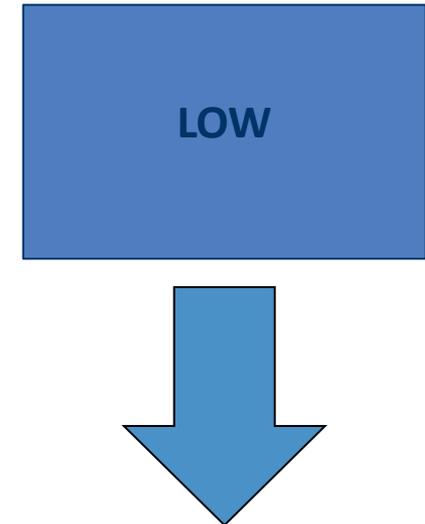
IT Risk Concepts – Control Risk (Continued):

Measuring Residual Risk

Residual Risk = the remaining risk after consideration of the control environment

Low

- Inherent risk/ part of doing business
- Manageable with minimal \$\$ impact



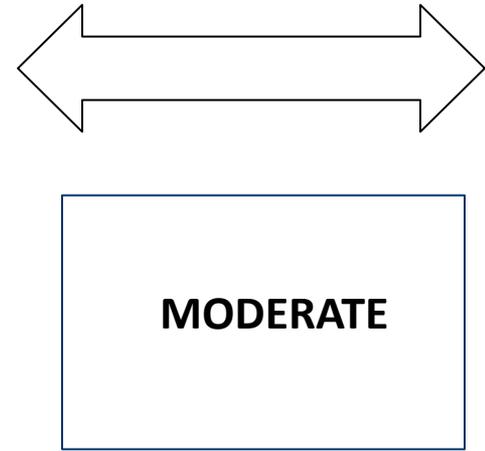
Performing Risk Assessment

IT Risk Concepts – Control Risk (Continued):

Measuring Residual Risk

Moderate

- Impacts customer data
- Significant effort to correct or recover
- Subject to regulatory scrutiny
- Subject to reputation damage



Performing Risk Assessment

IT Risk Concepts – Control Risk (Continued)

Measuring Residual Risk

High

- Customer \$ impact
- Loss of \$\$
- Regulatory / compliance violation
- Imminent problems expected



HIGH

Performing Risk Assessment

IT Risk Assessment Example

KEY PROCESS	INHERENT RISK				CONTROL RISK	RESIDUAL RISK
	People	Process	Technology	Aggregate Risk		
Hardware/Software	Low	Moderate	Low	Low	Low	Low
Fiserv ITI Core Application	Low	Moderate	Low	Low	Low	Low
Servers	Low	Moderate	Moderate	Moderate	Moderate	Moderate
Network Infrastructure	Moderate	High	High	High	Moderate	Moderate
Patch Management	Moderate	High	High	High	High	High
Website	Low	Low	Moderate	Low	Low	Low
Internet Banking	Low	Moderate	Moderate	Moderate	Low	Low
Imaging / IP	Low	Moderate	Moderate	Moderate	Low	Low
Wire Transfer / ACH	Low	Low	Low	Low	Low	Low

Summary Comments

Hardware / Software: Stable environment; core changed by vendor, IT personnel implements and maintains local IT environment.

Fiserv Premier Core Application: Stable environment; core changed by vendor and implemented by vendor; third party service bureau.

Servers: CIO and network administrator actively monitor and perform updates for all security related hotfixes and security patches on servers and workstations.

Network Infrastructure: Reliance is placed on vendors for configuration.

Patch Management: Network assessment results indicate limited issues with patch management.

Website: Limited scope of change to site; change requested to / made by vendor; need approval process for changes.

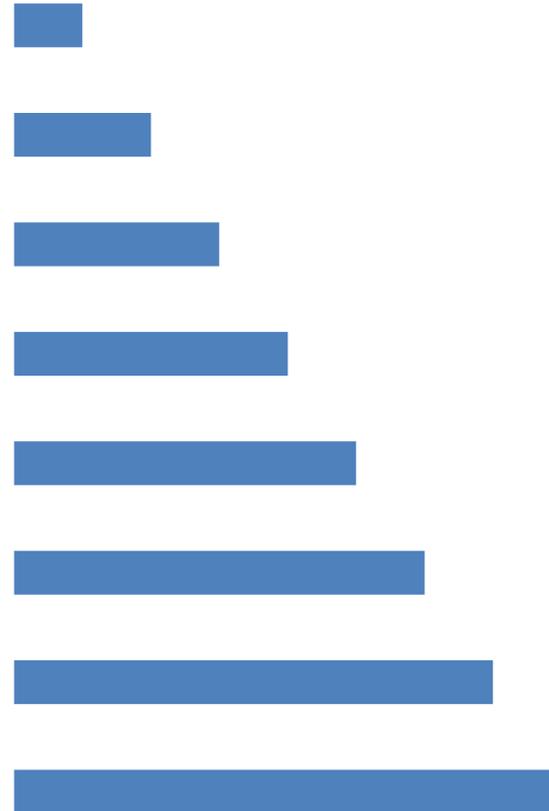
Internet Banking: Limited scope of change to application; changes made by vendor.

Performing Risk Assessment

Chronology of Technology

- Phones and fax machines
- ATMs and encryption
- Dumb terminals
- PCs
- Local area networks
- Server based applications/ Wide Area networks
- Email
- Voice response units
- Internet as a delivery channel
- Third part systems
- Convergence of digital voice and data
- Wireless
- Instant messaging
- Handhelds
- VOIP
- Social Networking
- Cloud computing
- TBD

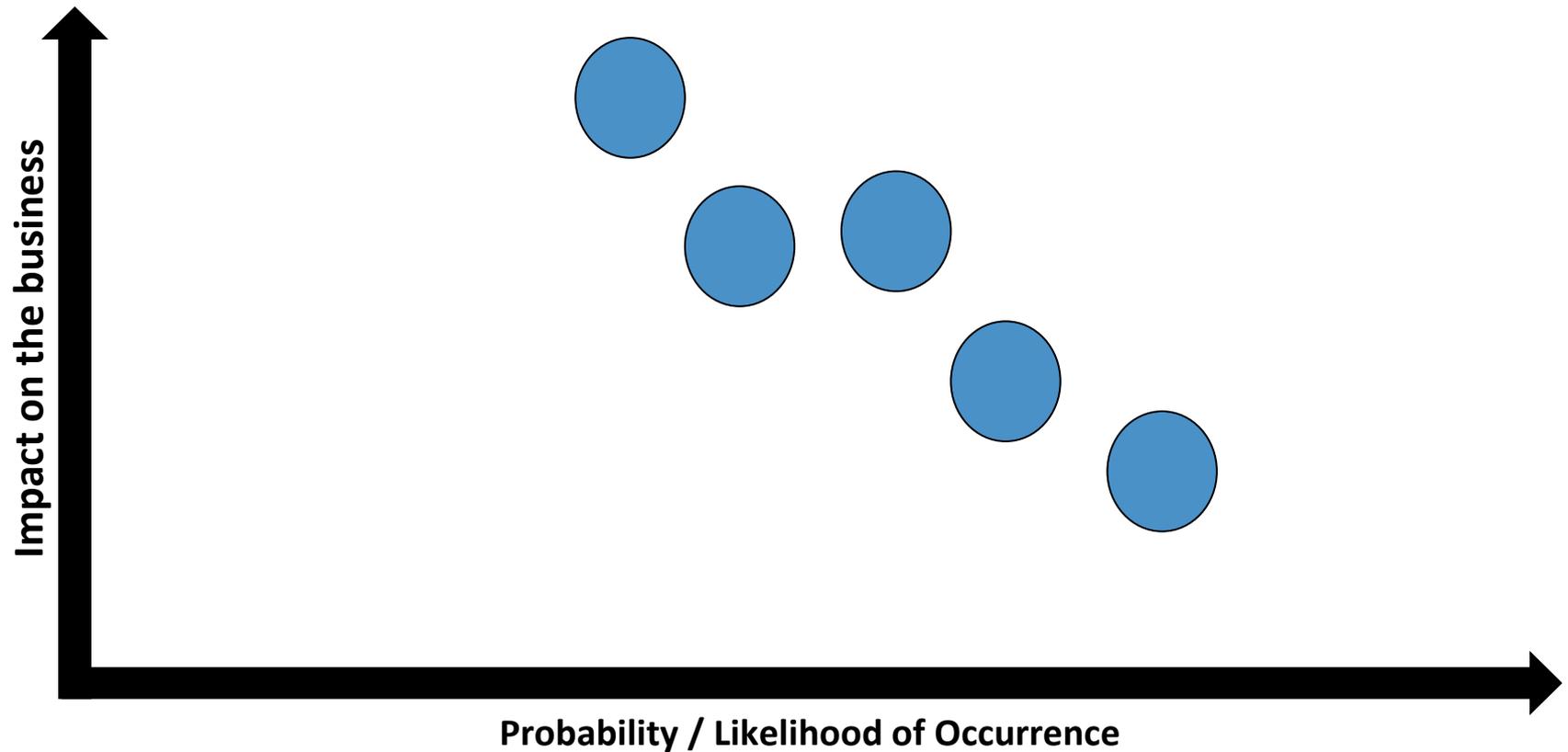
Level of Risk



Performing Risk Assessment

IT Risk Concepts

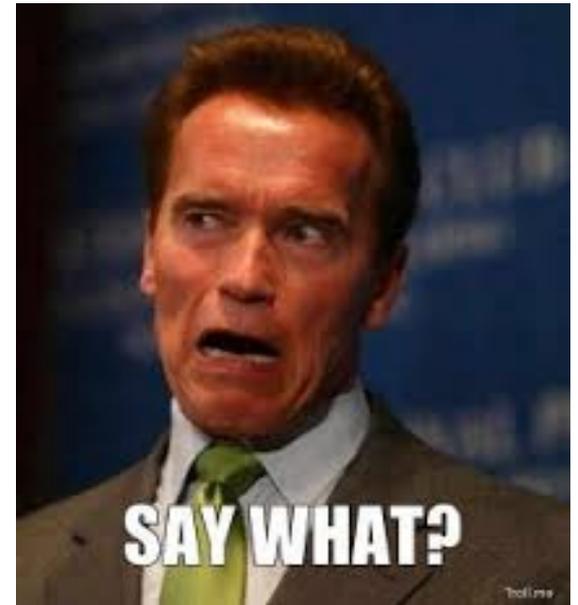
Areas of greatest risk
to your organization



Performing Risk Assessment

Risk and Control Frameworks for Commonwealth IT:

- SEC501-09 (IT Security Standard)
- SEC502.02.2 (IT Security Audit Standard)
- ISO 27001 and 17799
- NIST 800-53
- COBIT (Control Objectives for IT)
- ISACA
 - Risk IT Framework
- AICPA resources
- IIA resources
 - GTAG (Global Technology Audit Guides)
 - GAIT (Guide to the Assessment of IT Risk)



Performing Risk Assessment

How frequently is the risk assessment performed/updated?

- At least annually to support the internal audit plan
 - Dependent on the amount of planned or ongoing change

As needed:

- Technology risks to an organization change regularly
- New Vendors added
- News and current events considerations that affect risk

Interpreting Risk Assessment Results.....

What do I audit?

- The frequency the area would be tested is based on the residual risk
- Significant risk would result in audits being conducted annually
- Areas with less risk would result in audits being performed less often

The risks and degrees of change within the audit plan should be reviewed and discussed annually.

Summary - Observations

- Key component in understanding the environment
- Key to developing a cost effective overall audit plan
 - The nature, extent and timing of audit procedures
 - The areas or business functions to be audited
 - The amount of time and resources to be allocated to an audit
- Risk assessment is a dynamic / fluid process
- Overlap of risk assessments performed in other areas

Other Considerations for the IT Audit Plan

What other factors do I consider?

- External examiner prior comments, new guidance
- Management concerns
- Board / Audit Committee / Executive Management concerns
- Change events, conversions, implementations
- IT staff changes
- Internal audit skill sets
- Rotation of topics and areas

Other Considerations for the IT Audit Plan

What do I audit? Usual High Risk Areas

- Security configurations
- Network recovery and business unit planning
- Policies and procedures
- Change management processes
- Logical security
- Intrusion detection capabilities, network management
- Vendor management

DHG

DIXON HUGHES GOODMAN LLP

How To Make An Audit Effective “For All Parties”

Potential IT Audit Areas/IT Audit Coverage

Areas that are often covered as part of an IT Audit can include:

- IT Governance
- Physical Security
- Network Administration
- Network Vulnerability Assessments – how often? Int./Ext.?
- Business Continuity Plan / Disaster Recovery
- Environmental
- Service Provider Management (Vendor Management)
- Spreadsheets (used for financial reporting / key management decision-making)
- Desktop Management
- Information Security
- Change Management

Potential IT Audit Areas/IT Audit Coverage

Areas that are often overlooked

- IT Controls within processes (accounting, purchasing, etc.)
- Spreadsheets used for financial reporting / key management decision-making
- External data / file transfer – email encrypted, SFTP
- Specialty third party processing (backup solutions, statement printing, data mining)

How the IT Department Can Benefit from an Audit

Ways that Internal Audit can provide a benefit to the IT Department can include the following.....

- Internal Audit reports directly to Executive Management and therefore can help bring attention to issues that may impact the performance of critical day-to-day business operations, such as.....
 - The need for more software licenses or servers required to support growth in business operations.
 - Under or over staffed areas of the IT Department that need to support certain business areas.
 - Supporting antiquated or unsupported technology that may present certain threats or vulnerabilities to the agency's sensitive data. In addition, supporting antiquated systems can also prove to be costly to an agency or lead to the misuse of available resources.

Ways that Internal Audit can provide a benefit to the IT Department can include the following.....

- Internal Audit reports directly to Executive Management and therefore can help bring attention to issues that may impact the performance of critical day-to-day business operations, such as.....
 - Trainings or specialized staff to help support technology initiatives being pursued by your Agency.
 - Changes to applications/infrastructure to better suit the needs of the Agency or the security/ease of operations/maintenance for the IT Department.
 - More funds for key projects/initiatives where goals and budget expectations were designed too lean or without enough cushion or where on-going maintenance was not adequately addressed in the implementation phase of a project.



DHG

DIXON HUGHES GOODMAN LLP

Appendix A: IT Audit Coverage/Program – Examples of Key Controls and Common Audit Findings

IT Governance – Key Controls

- Key Controls
 - Organization charts, current job descriptions, and current operating policies and procedures
 - Organization structure is in place to support effective monitoring of activities and provide segregation of duties between IS staff and users.
 - Proper levels of responsibilities that are clearly defined for adequate segregation of duties.
 - IT policies and procedures developed to provide guidance to each State Agency regarding information security, data integrity and information privacy
 - IT budgeting

IT Governance – Key Controls

- Key Controls (continued)
 - IT personnel hiring and performance / training / cost requirements
 - Documented evidence of reporting to the Board / Executive Management involvement
 - Long range IT planning / strategy
 - Job descriptions are in place to outline tasks / responsibilities of IT personnel.

IT Governance – Common Findings

- Common Findings / Observations
 - IT Strategic Plan and IT Budget have not been developed.
 - Policies and Procedures are not formally adopted by the Board of Directors or Executive Management at each State Agency.
 - Policies and procedures – coverage of all key requirements is lacking (wireless, encryption, monitoring tactics, etc.)
 - IT Strategic Plan does not provide specific information that would allow management to planning
 - Technology Committee is not in place or Technology Committee meetings are not taking place on a regular basis
 - BOD can review minutes

Physical Security – Key Controls

- Key Controls
 - Locating servers in locked rooms to which access is restricted
 - Building access, key locations, and server room access
 - Access to facilities is restricted to authorized personnel and requires appropriate identification and authentication
 - Physical access is reviewed on a periodic basis to ensure appropriate access exists.
 - Terminated employee physical access is removed on a timely basis
 - Visitor / contractor access to the facilities is monitored and logged to ensure appropriateness

Physical Security – Common Findings

- Common Findings / Observations
 - Unauthorized access to server room
 - Terminated users have badge access to facility
 - Branch servers are not in secure areas
 - Controlling visitor access
 - Branch security

Network Administration – Key Controls

- Key Controls
 - Administrative access to network devices is limited to authorized individuals and secured by strong passwords that are changed periodically.
 - Laptops housing financial data are configured / encrypted to prevent unauthorized access if lost / stolen.
 - Mobile devices housing financial data are configured to prevent unauthorized access.
 - Individual passwords are required for each network user. Network passwords are configured in accordance with the organization's policies and current industry standards.
 - Security administration monitors network device security logs. Any identified security violations are subject to formal incident response procedures.

Network Administration – Common Findings

- Common Findings / Observations
 - Network device user ID and passwords are shared – limitation of most devices
 - Mobile devices have weak controls / limited security – need password – look into remote HD wipe
 - Review of network device logs not occurring or documented
 - Storage of network device logs – size requirements

- **Key Controls**

- External Vulnerability Assessment and Penetration Testing**

- Identify and assess network security vulnerabilities on all external facing devices within the infrastructure used to support web-enabled activities (Internet access to the network, Internet-based transactions, email servers, and remote access)

- Manual Mode**

- Information Gathering

- Automated Mode**

- Scan Identified Segments (Active Exploration)
 - Research exploits for vulnerabilities identified
 - Exploitation of known vulnerabilities

- **Key Controls**

- Internal Vulnerability Assessment**

- Identify and assess vulnerabilities associated with the infrastructure that makes up the internal network.

- Manual Mode**

- Information Gathering

- Automated Mode**

- Scan Identified Segments (Active Exploration)
 - Research exploits for vulnerabilities identified
 - Exploitation of known vulnerabilities

- Common Findings / Observations
 - A network vulnerability assessment has not been conducted
 - Critical findings have not been remediated by management
 - Patch management issues
 - Data bases running in the background not secured
 - Many vulnerabilities a direct result of personnel not performing needed tasks
 - Hardware / software additions implemented by vendors

Business Continuity Plan / DR – Key Controls

- **Key Controls**

- Testing of the BCP plan on an annual basis, or more frequent
- BCP plan is documented, evaluated by institution management, independently reviewed by an internal and / or external audit function, and reported to the Board
- Data record retention plan – individual states have guidance
- Risk assessment and BIA methods are utilized to establish interruption exposures, their probability and impact, and remediation alternatives. BCP utilizes risk analysis to determine the strategy and recovery plans

- **Key Controls (continued)**
 - Critical applications and supporting platforms have been identified
 - Appropriate facilities have been identified and plans are in place to support the interim processing and restoration of computer operations according to the priorities established in the BCP.
 - Staff responsibilities, notification, substitution, and access procedures are in place to permit the timely assembly of staff and the commencement of interim and/or restoration procedures.
 - The plan is distributed on a need-to-know basis, is securely stored in soft and hard copy, and can be obtained from multiple locations in the event that the primary storage location has been affected by the incident.

- **Key Controls (continued)**
 - Involvement of the Board and senior management
 - Backups are performed and reviewed on a regular basis
 - Backup tapes are rotated off-site on a regular basis

Network Vulnerability Assessments – Common Findings

- Common Findings / Observations
 - Management has not performed a Business Impact Assessment – BIA should be considered all departments and business functions
 - Still IT based – hasn't expanded to business unit resumption
 - Newer network components have not been included in planning and testing
 - Connectivity of branch network to recovery site not planned or tested
 - Focus more on availability versus disaster recovery – cheaper bandwidth and servers have led to third party solutions
 - Backup tapes are not encrypted prior to being transported offsite storage or testing. – password protected?

Environmental – Key Controls

- **Key Controls**

- Environmental controls are in place in the data center / computer room
 - Fire detection and suppression equipment
 - Generator and UPS devices
 - Independent heating / cooling and humidity controls exist – separate HVAC
 - Monitoring of heating and cooling devices
 - Raised flooring / higher level floors
- Maintenance and testing is completed regularly on fire suppression, generator, and UPS devices

Environmental – Common Findings

- Common Findings / Observations
 - The server room storing critical computer equipment is located in an area containing a water pressurized fire suppression system that could potentially cause irreparable damage to electronic equipment in the event of an accidental discharge.
 - Management does not have a generator in place that would provide for continuous operations in the event of an extended regional or local power outage as a result of a natural disaster
 - Lack of testing of fire suppression equipment, UPS, generators

Service Provider Management – Key Controls

- **Key Controls**

- Annual vendor management assessment
 - Risk Assessment
 - Financial statement review
 - Insurance coverage
 - Meeting SLA agreements – ongoing marketing
 - Contract review
 - Business continuity
- Review of SAS 70 reports for key providers
- Review of User Control Considerations (UCC's)
- Selection of new vendors for outsourced services in performed in accordance with the organizations vendor management policy to ensure vendor evaluations are performed prior to entering into contracts.

Service Provider Management – Common Findings

- Common Findings / Observations
 - Management has not obtained the SAS70 audits for all service providers that support core business processing / user control considerations have not been reviewed or documentation is poor
 - No formal processes in place to evaluate vendor performance on an annual basis.
 - Performance metrics/ SLA being met
 - Financial assessment
 - Insurance policy review
 - Risk Assessment
 - Contract management
 - DR reviews / SAS 70s / audits
 - Due Diligence in selecting a service provider
 - Vendor contract review by legal council
 - Risk Assessment
 - Financial

Critical Spreadsheets – Key Controls

- **Coverage**

- Only spreadsheets used for financial reporting / key management decision making

- **Key Controls**

- The Bank has identified all critical spreadsheets and maintains an up-to-date inventory of spreadsheets that have been identified as being key for financial reporting purposes
- Access to critical spreadsheets is appropriately restricted
- Access to critical applications is restricted by usage of approved, unique user IDs. Password settings should be set to minimize risk of unauthorized access

Critical Spreadsheets – Key Controls

- **Key Controls (continued)**

- Management monitors the appropriateness of user access on a periodic basis by reviewing current access reports.
- Critical spreadsheet backup files are created daily
- Backup files are rotated off-site regularly to an environmentally and physically secure location
- Changes to spreadsheets
 - Formulas
 - Functionality
 - Cells



Critical Spreadsheets – Common Findings

- Common Findings / Observations
 - Critical spreadsheets have not been identified
 - Lack of password controls around spreadsheet access
 - Changes to spreadsheets occur without authorized review
 - Spreadsheets are stored on central drive with unlimited access
 - Spreadsheets are not backed up on a regular basis

Distributed Applications – Key Controls

- **Key Controls**

- Data origination controls – properly authorized and approved
 - User IDs and passwords
 - Prohibiting IT personnel from authorizing, preparing, entering or correcting transactions
 - Reviewing exception audit trails
 - Reviewing security access rights
- Input controls
 - User controls over regular data, file maintenance, inquiry and error correction transactions
 - Authorizations, segregations of duties, audit trails data edits performed, balancing and verification procedures, forms
 - Input verification and error detection, system edit checks
- Processing controls
 - Balancing, reconciliations
- Output controls
 - Output distribution – authorized users only

- Common Findings / Observations
 - Limited permissions on file servers
 - Multiple administrative accounts
 - Security configurations are not matching Bank Information Security policy requirements
 - Access reviews are not being completed – scope of the application reviews are not in depth enough

Desktop Management – Key Controls

- **Key Controls**

- Equipment acquisition and deployment
- Hardware and software problem reporting and resolution
- Administrative processes are in place for technology asset management to include up-to-date inventory of software and hardware – Hardware and software asset custodianship
- Software license management
- Desktop performance monitoring and measurement
- LAN and desktop applications implementation and version control

- **Common Findings / Observations**
 - Equipment and hard drive disposal
 - Standard images / configurations not utilized for desktops
 - Patch management not current
 - Antivirus not implemented / current
 - Laptops not being encrypted

- **Key Controls**

- Sufficient evidence is maintained to demonstrate management / HR approval of access requests. (new hires, terms, changes)
- Terminated user access is revoked upon employee separation.
- Core application and network access reviews are performed annually to ensure access levels align with employee job responsibilities.
- Individual passwords are required for each network and core application user. Passwords are configured in accordance with the organization's policies and current industry standards.
- Antivirus software is implemented for servers, desktops, and laptops. Definitions are updated daily.

- **Key Controls (continued)**

- Remote access is limited to authorized vendors
 - Remote sessions disabled while not in use
 - Strong security parameters (minimum of 8 characters, password expiration, complexity) are required for remote access authentication
 - Remote access by vendors is captured in system audit trails
- Remote employee access is limited to authorized employees
 - Limited to authorized employees only
 - Strong security parameters (minimum of 8 characters, password expiration, complexity) are required for remote access authentication.
- Administrative rights over the network and core application is limited to authorized personnel.
- Default administrator passwords have been changed since system installation.

- **Key Controls (continued)**

- Reports which record unsuccessful attempts to gain access to the network perimeter are routinely reviewed
- Windows audit logs are enabled and event logs are routinely reviewed
- Reports which record unsuccessful attempts to gain access to the core application are routinely reviewed.
- Virus detection software is installed on all PCs and servers. Antivirus definitions are installed to computers as made available by the vendor.
- Encryption and data security (storage and in transit)
 - Encryption is in place for sensitive e-mail correspondence.
 - Laptop hard drives containing sensitive or confidential information are encrypted.
- Acceptable use policy

- **Common Issues / Observations**
 - Company's internal management of passwords
 - Administrative rights to too many personnel
 - Poor server security over internal access rights
 - Poor authentication requirements / settings
 - Too much access by network support vendors

Change Management – Key Controls

- **Key Controls**

- Change management policies and procedures are in place for emergency and standard core financial applications and Network changes, Operating System software and hardware changes, and patch management.
- Only authorized personnel can migrate program changes into production.
- Core financial application upgrades, releases, and code changes are subject to formal change management procedures including approval and testing. Segregation of duties is in place.
- Parameter and maintenance changes to core financial applications are subject to formal change management procedures. Segregation of duties is in place.

- **Key Controls (continued)**

- Network configuration changes are documented and subject to formal change management procedures including approval and testing.
- Operating System software and Hardware changes are documented and subject to formal change management procedures including approval and testing.
- Patches for operating systems are subject to formal change management procedures including approval and testing. Process is in place to ensure that all Windows-based Servers and PCs are updated regularly with critical patches.

- **Common Findings / Observations**

- Change management procedures are not documented
- Need to track changes planned and made – are users aware of upcoming changes?
- Proper segregation of duties is not maintained for programmers in application – programmers have access to both the test and production environments. Changes to source code can be implemented into the production environment by the same individual who made them without recording the changes that have occurred.
- Program changes are installed to production without being tested.
- Parameter changes are not documented to evidence independent review and approval of changes / made under dual control

Conclusion

- **IT risk assessment process drives the IT audit plan**
- **IT risks change frequently** – Update the risk assessment as risks, technologies, and business environment / processes change
- **The frequency and scope of IT internal audit plan is driven by many factors**
 - Risk
 - Management
 - Regulators
 - Changes
 - New Guidance

Contact Information:

Chadam Hover, CISA
Phone: 804.282.7636
Risk Advisory Services
Chadam.Hover@dhgllp.com

Peter Tsengas, CISA, CISM
Direct: 804.474.1293
Risk Advisory Services
Peter.Tsengas@dhgllp.com



Verizon Data Breach Report

**Bhavesh Chauhan,
Verizon**

August 5, 2015



2015 DATA BREACH INVESTIGATIONS REPORT

Understand the risks you face
and prioritize your defenses

HOSPITALITY
EDUCATION
PUBLIC SECTOR
ACCOMODATION
FINANCIAL SERVICES
RETAIL
ENTERTAINMENT
PROFESSIONAL
MANUFACTURING
TECHNOLOGY
ADMINISTRATIVE
TRANSPORTATION

Bhavesh Chauhan, CISSP, CISA, CISM
Principal - Security Engineering
bhavesh.chauhan@verizon.com

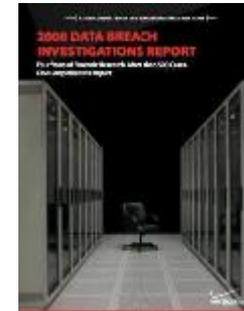


DATA BREACH INVESTIGATIONS REPORT

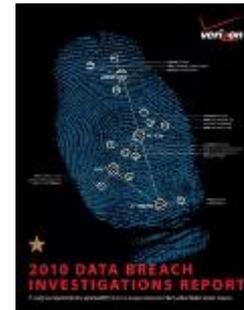
THERE'S ONLY ONE DATA BREACH INVESTIGATIONS REPORT (**DBIR**).

- THE LEADING DATA SECURITY REPORT **FOR EIGHT YEARS.**
- **MILLION'S OF DOWNLOADS / WIDELY USED / REFERENCED.**
- TURNS DATA INTO **USEFUL, ACTIONABLE INFORMATION.**

2008



2009



2010



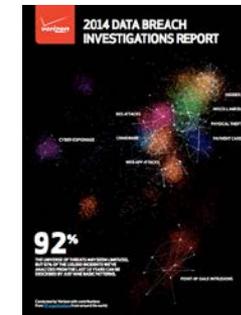
2011



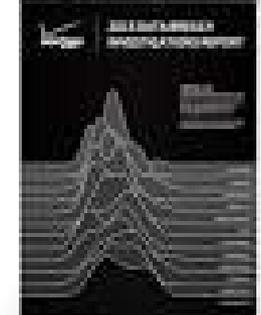
2012



2013



2014



2015

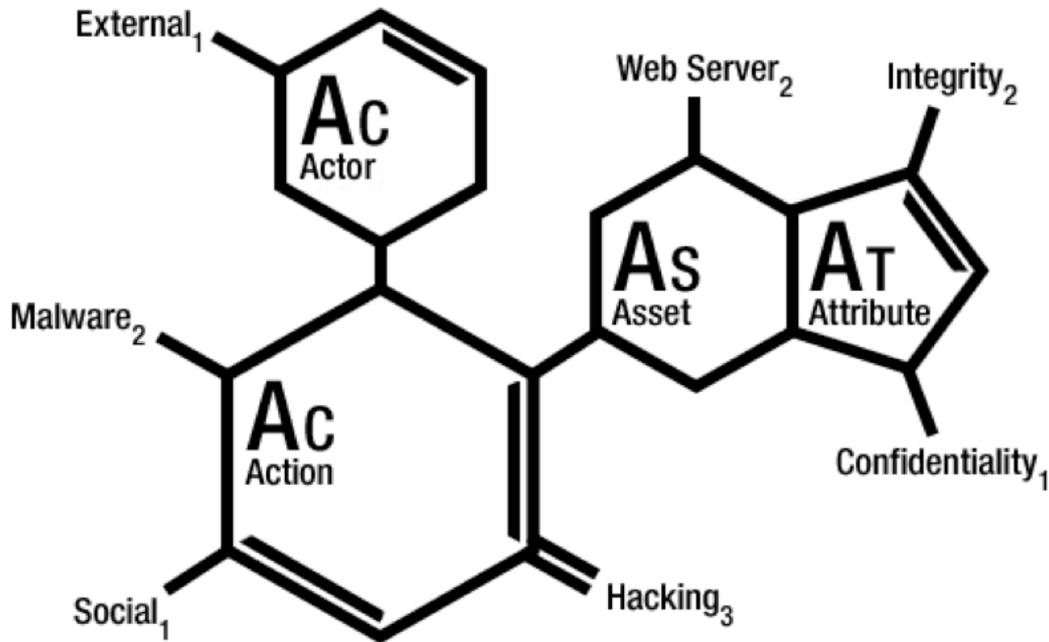


Some of the 70 Contributors from around the world



Our Framework

The Vocabulary for Event Recording and Incident Sharing (VERIS)



Actor – Who did it?

Action – How'd they do it?

Asset – What was affected?

Attribute – How was it affected?

Documentation, classification examples, enumerations: <http://veriscommunity.net/>



Contributors, Coverage & Corpus



70
CONTRIBUTING
ORGANIZATIONS

79,790
SECURITY INCIDENTS

2,122
CONFIRMED
DATA BREACHES

61
COUNTRIES
REPRESENTED¹



Security Incidents by victim industry & organization size - 2015

INDUSTRY	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services(52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31-33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44-45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48-49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047



Victim Demographics

NUMBER OF SECURITY INCIDENTS CONFIRMED DATA LOSS

INDUSTRY	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services(52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31-33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44-45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48-49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

70%
of attacks show
secondary victim

75%
spread from
victim 0..1 within
one day



2014 Security Incident - vs. Data Breach

Figure 2.
Number of security incidents by victim industry and organization size, 2013 dataset

Industry	Total	Small	Large	Unknown
Accommodation [72]	212	115	34	63
Administrative [56]	16	8	7	1
Agriculture [11]	4	0	3	1
Construction [23]	4	2	0	2
Education [61]	33	2	10	21
Entertainment [71]	20	8	1	11
Finance [52]	856	43	189	624
Healthcare [62]	26	6	1	19
Information [51]	1,132	16	27	1,089
Management [55]	10	1	3	6
Manufacturing [31,32,33]	251	7	33	211
Mining [21]	11	0	8	3
Professional [54]	360	26	10	324
Public [92]	47,479	26	47,074	379
Real Estate [53]	8	4	0	4
Retail [44,45]	467	36	11	420
Trade [42]	4	3	0	1
Transportation [48,49]	27	3	7	17
Utilities [22]	166	2	3	161
Other [81]	27	13	0	14
Unknown	12,324	5,498	4	6,822
Total	63,437	5,819	47,425	10,193

For more information on the NAICS codes [shown above] visit:
<https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012>

Source: verizonenterprise.com/DBIR/2014

Figure 3.
Number of security incidents with confirmed data loss by victim industry and organization size

Industry	Total	Small	Large	Unknown
Accommodation [72]	137	113	21	3
Administrative [56]	7	3	3	1
Construction [23]	2	1	0	1
Education [61]	15	1	9	5
Entertainment [71]	4	3	1	0
Finance [52]	465	24	36	405
Healthcare [62]	7	4	0	3
Information [51]	31	7	6	18
Management [55]	1	1	0	0
Manufacturing [31,32,33]	59	6	12	41
Mining [21]	10	0	7	3
Professional [54]	75	13	5	57
Public [92]	175	16	26	133
Real Estate [53]	4	2	0	2
Retail [44,45]	148	35	11	102
Trade [42]	3	2	0	1
Transportation [48,49]	10	2	4	4
Utilities [22]	80	2	0	78
Other [81]	8	6	0	2
Unknown	126	2	3	121
Total	1,367	243	144	980

Small = organizations with less than 1,000 employees,
 Large = organization with 1,000+ employees

Source: verizonenterprise.com/DBIR/2014



2015 VERIZON DATA BREACH INVESTIGATIONS REPORT

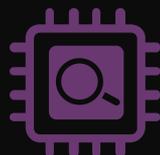
**What are
the threats?**



Understand the threats



Crimeware



Cyber-espionage



Denial of service attacks



Insider and privilege misuse



Miscellaneous errors



Payment card skimmers



Physical theft and loss



Point-of-sale intrusions



Web app attacks

Our 9 incident patterns make it easier



Incidents by pattern

Three patterns account for **75% of all security incidents**



Misc errors



Privilege misuse



Crimeware





Breaches by pattern

Just three patterns accounted for **66% of data breaches.**

29%



POS attacks

19%



Crimeware

18%



Cyber-espionage



2015 VERIZON DATA BREACH INVESTIGATIONS REPORT

**What are the
biggest threats to
your organization?**



Finance

3 patterns =
62%

of incidents in
financial
services
companies



Web app attacks



Crimeware



DoS attacks





Public sector

3 patterns =
80%

of incidents in
the public
sector



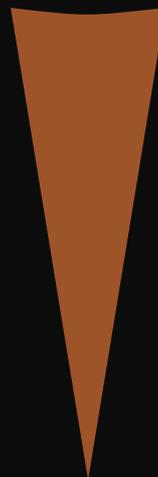
Misc errors



Physical theft/loss

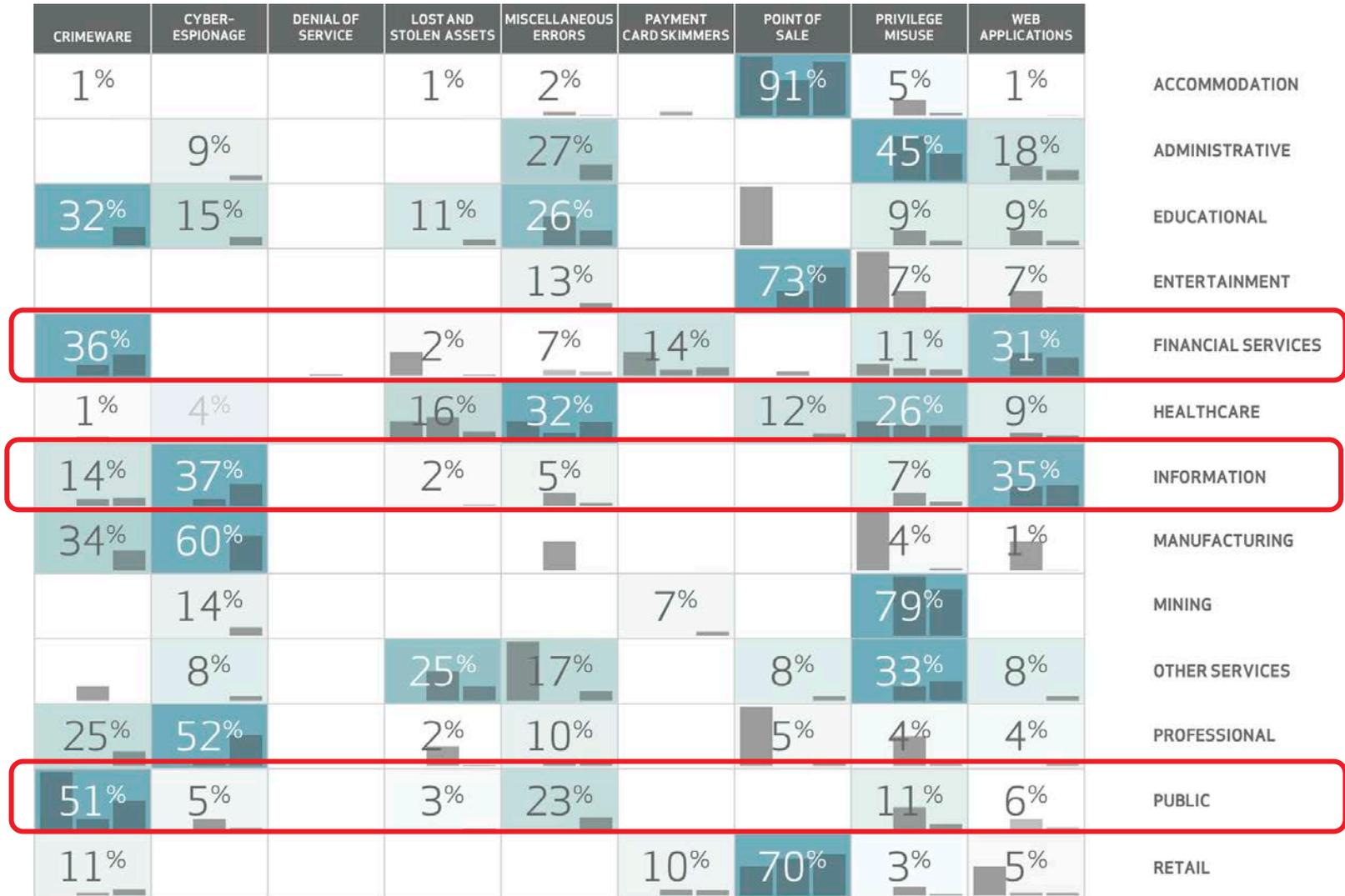


Privilege misuse





The Nefarious Nine Data Breaches Only





The Threat Actors

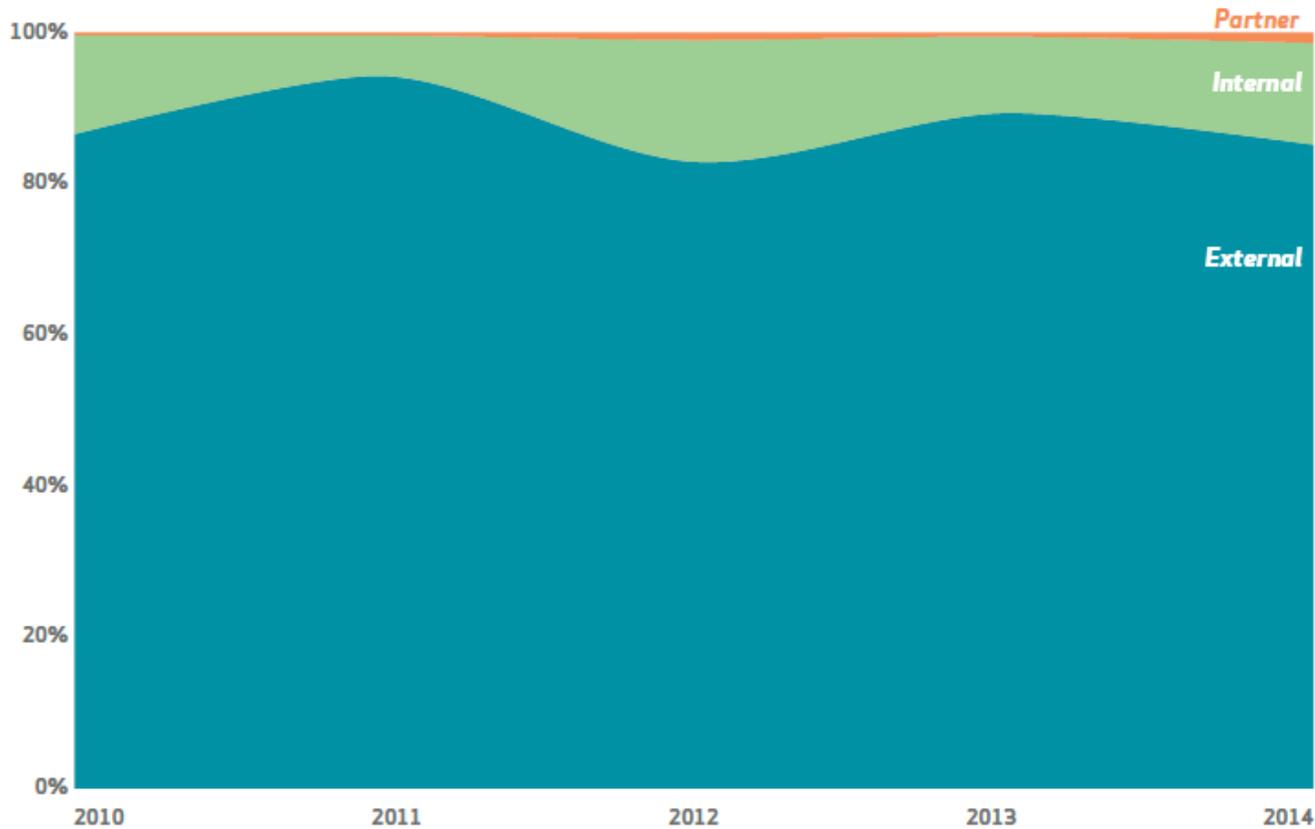


Figure 3.

Actor categories over time by percent of actors



Top 20 varieties of threat actions over time

5 Years of Threat Actions: RAM Scrapers and Keyloggers





Common vulnerabilities dominate

We saw more than **7 million**
vulnerabilities exploited in 2014

But just 10 accounted for **97% of attacks**

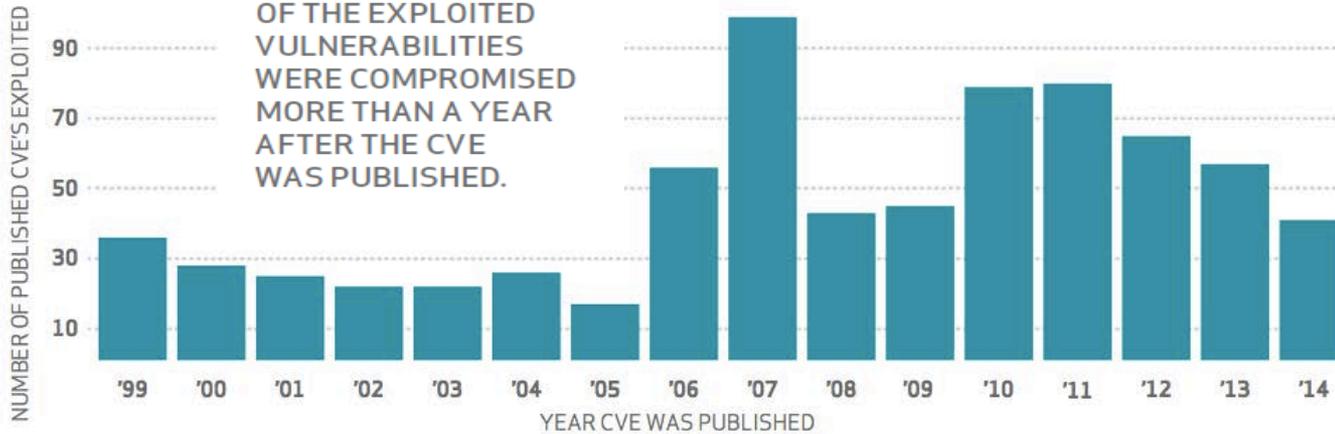
We found more attacks dating back to 2007 than from any year since. And most attacks exploited vulnerabilities where a patch has been available for months, often years.



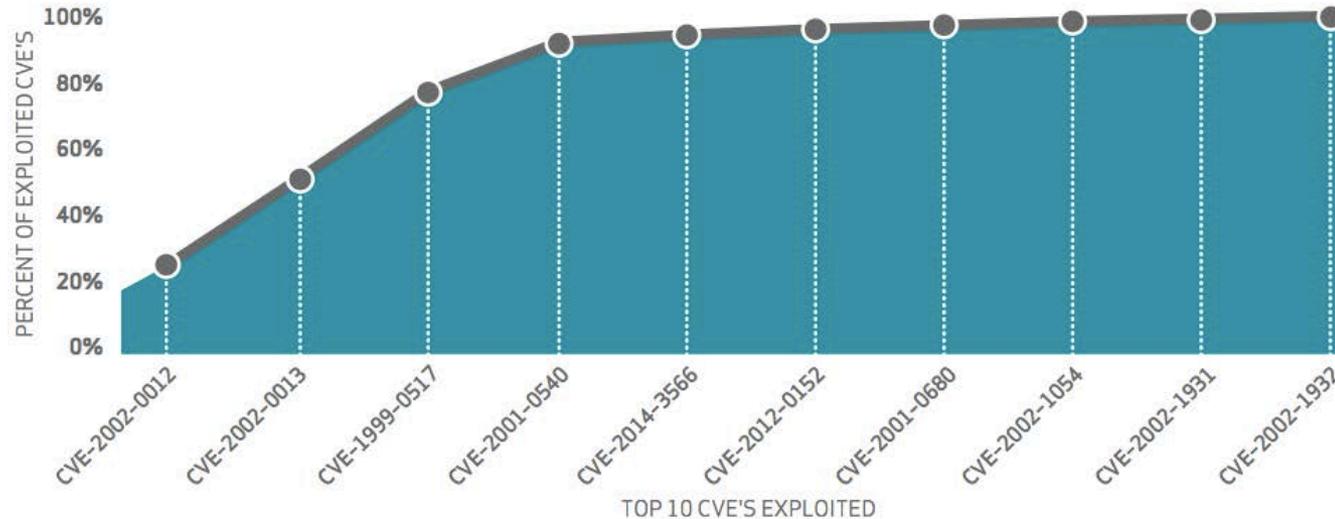
Common Vulnerabilities Dominate

99.9%

OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED.



7 million vulnerabilities exploited in 2014

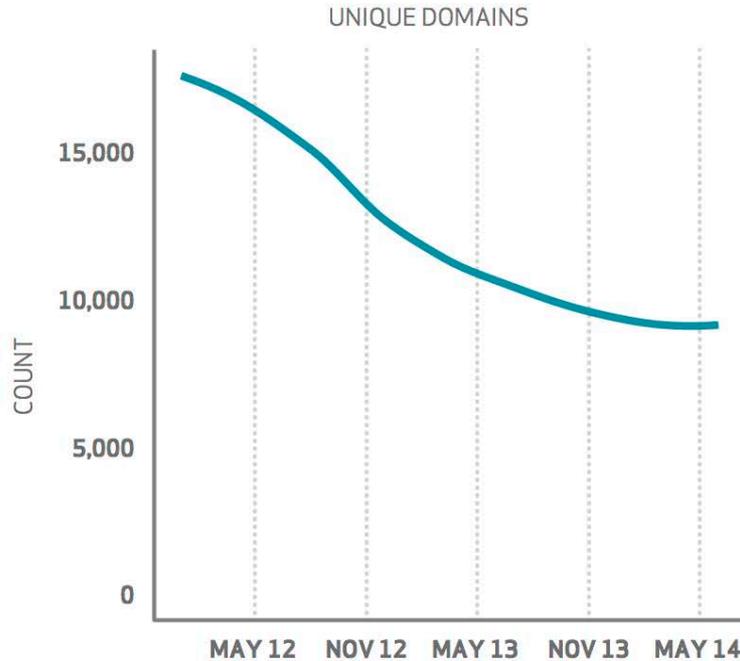


99% compromised more than a year after CVE

10 CVEs account for 97% of 2014 exploits



Phishing Remains a Threat



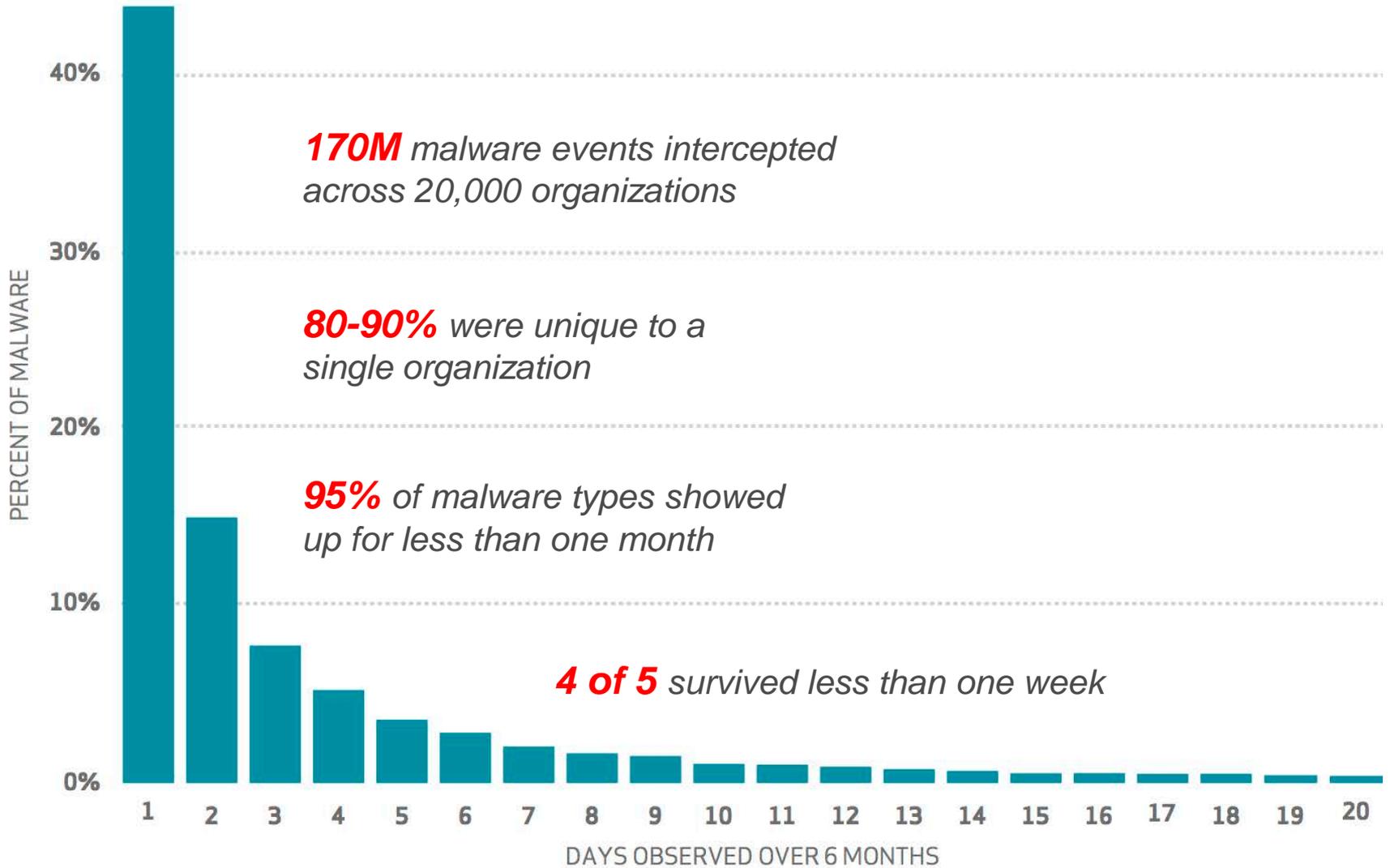
23%
of recipients opened
phishing messages

11%
of recipients clicked
on attachments

82 seconds
from start of a phishing
attack to first bite



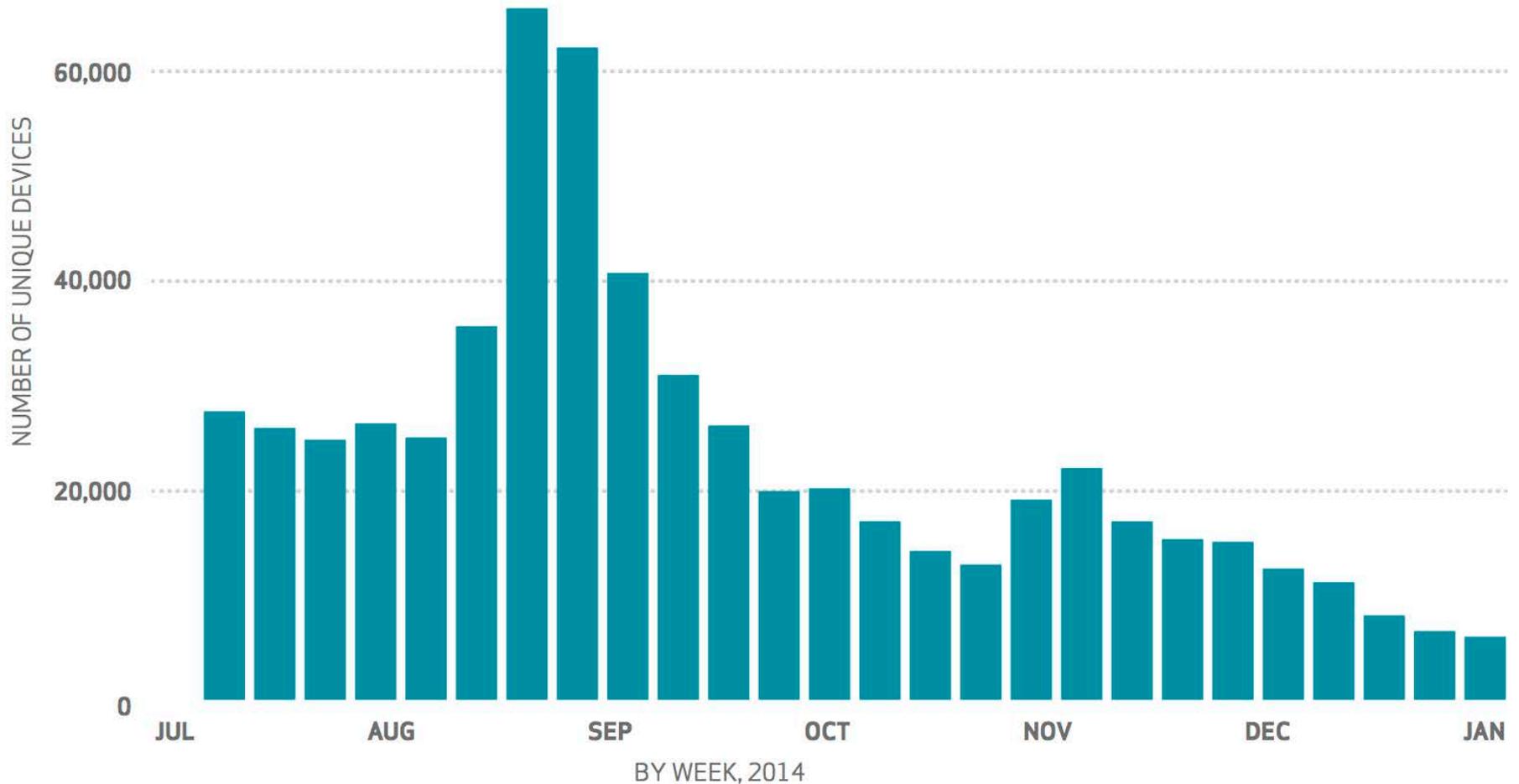
Malware Sophistication





Overstated Threat of Mobile

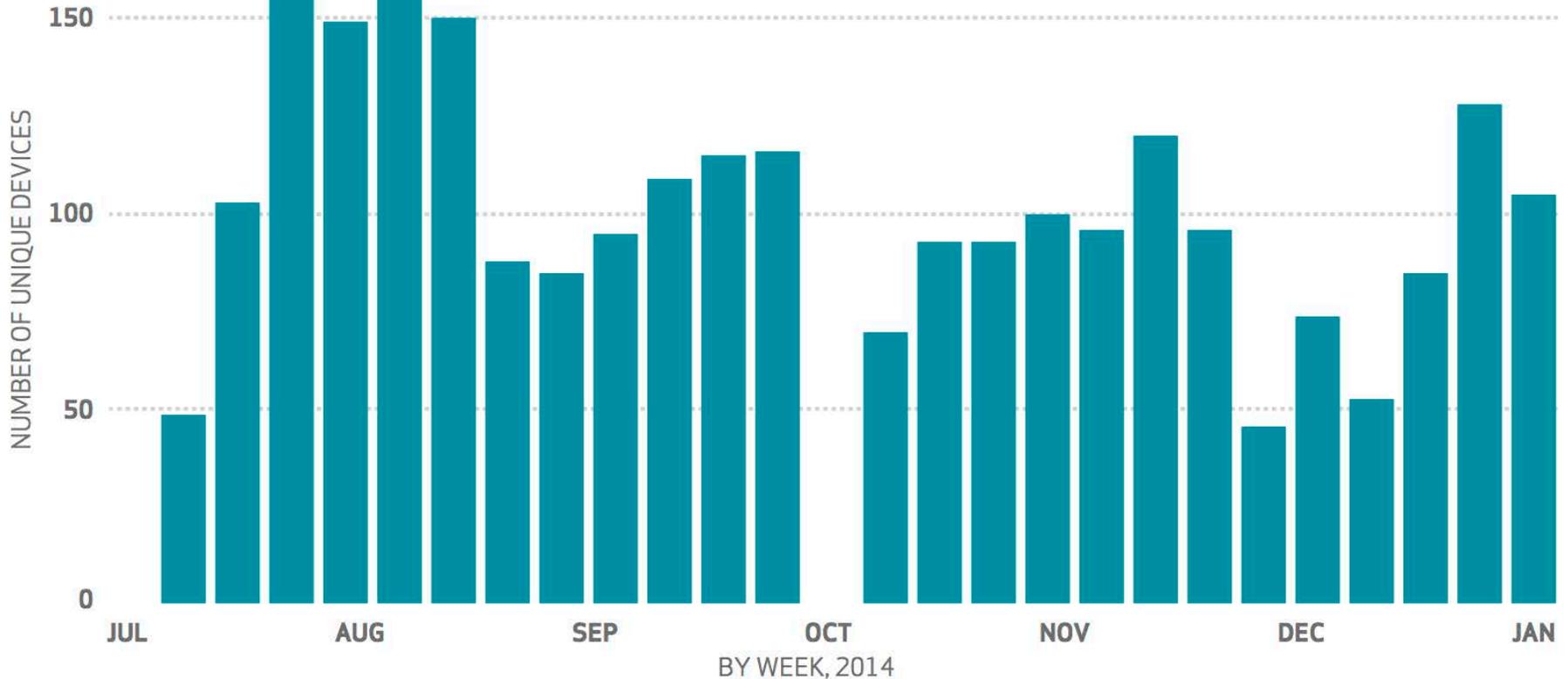
Count of Detected Infections





Overstated Threat of Mobile Non-Adnoyance Malware

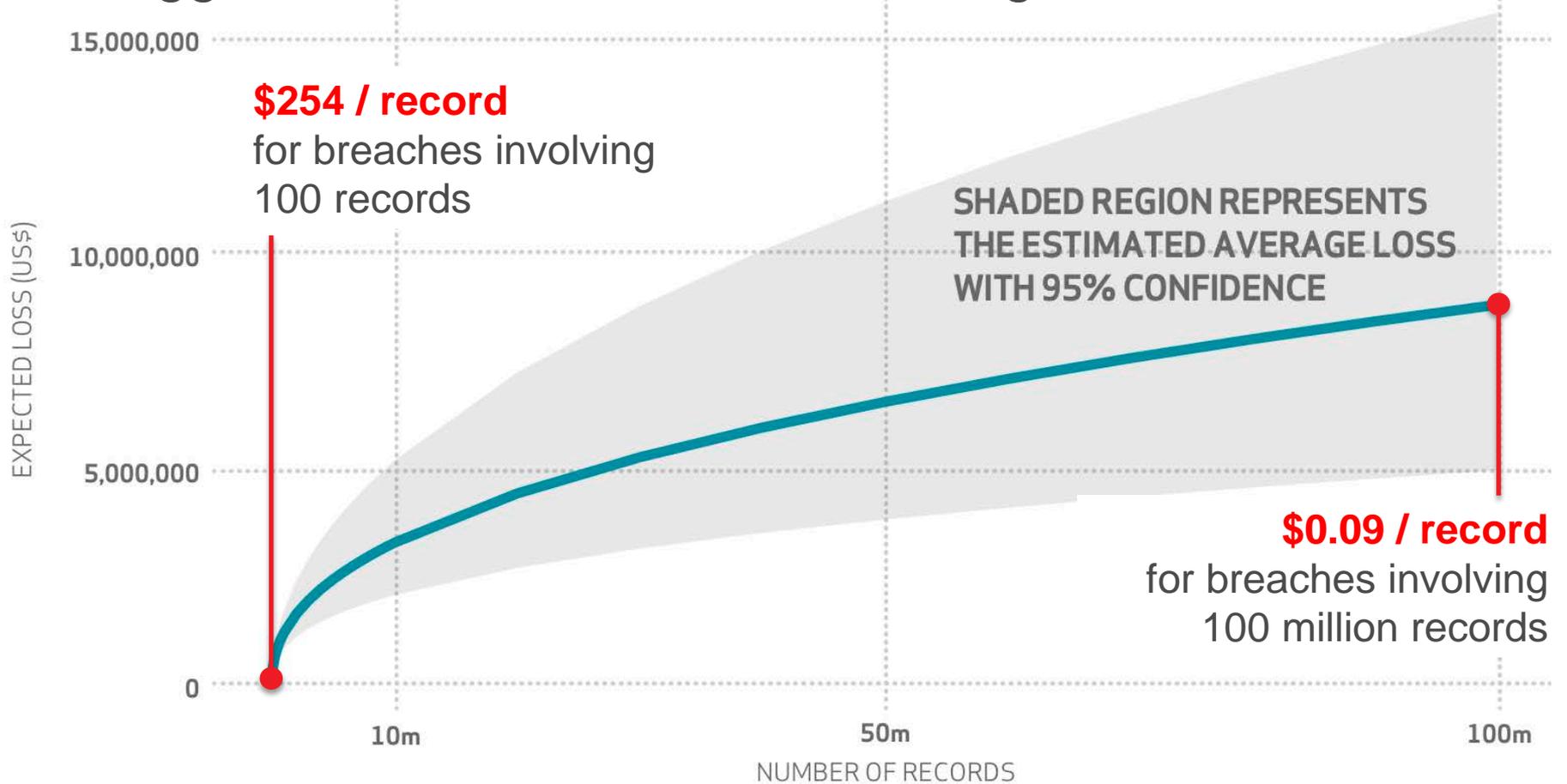
<0.03% of mobile devices
are affected by high-impact
malware each year





The Cost of a Breach

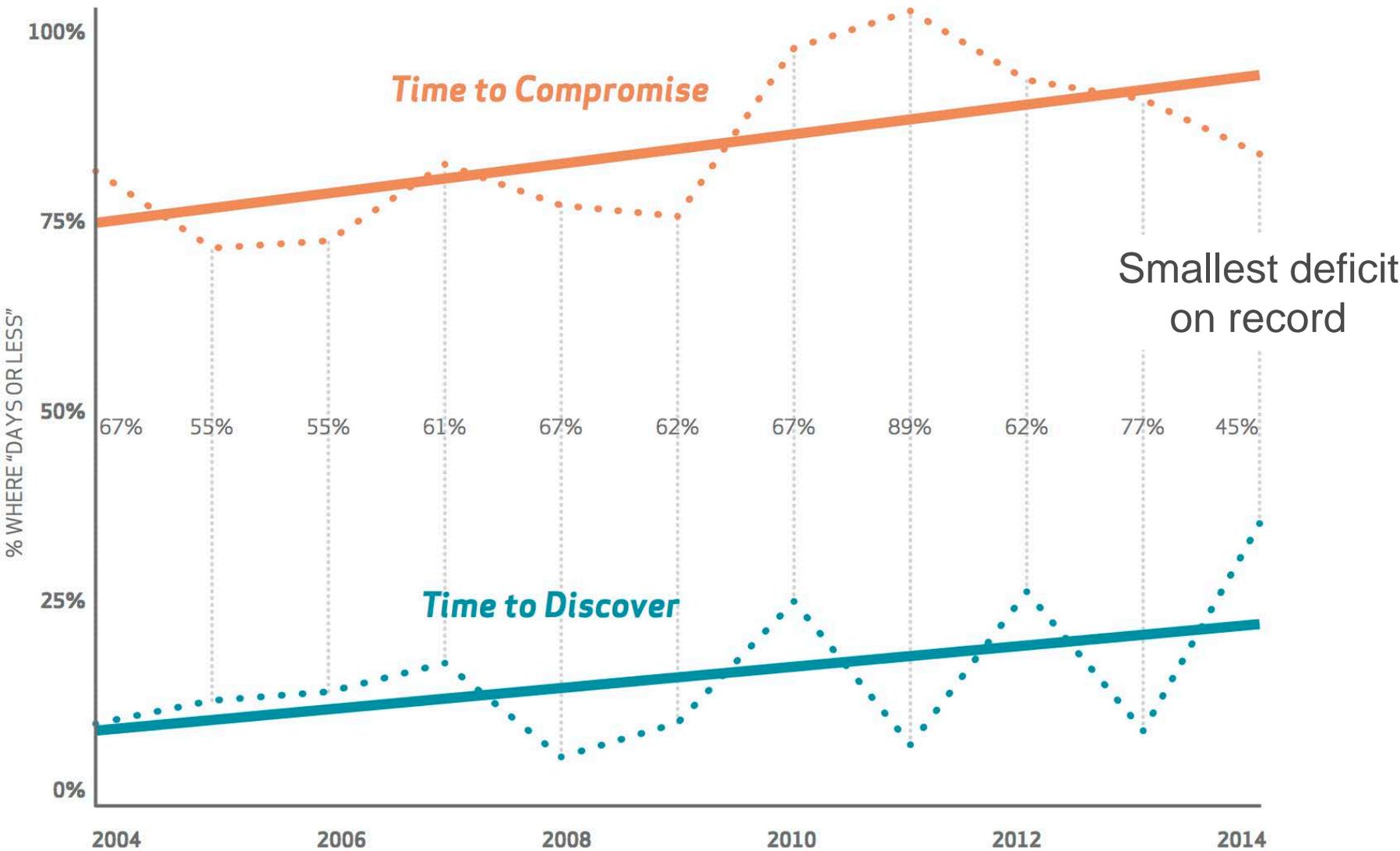
Bigger breaches cost more, but the growth isn't linear



<http://www.netdiligence.com/> - Cyber Liability & Data Breach Insurance Claims study



The Detection Deficit





Recommendations

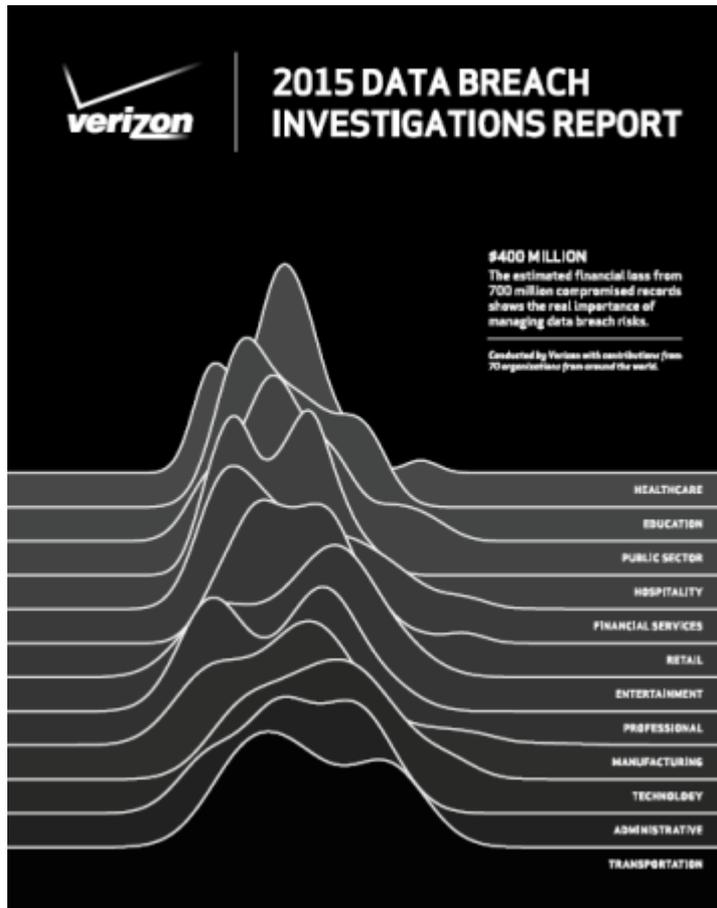


CSC	DESCRIPTION	PERCENTAGE	CATEGORY
13-7	2FA	24%	Visibility/Attribution
6-1	Patching web services	24%	Quick Win
11-5	Verify need for Internet-facing devices	7%	Visibility/Attribution
13-6	Proxy outbound traffic	7%	Visibility/Attribution
6-4	Web application testing	7%	Visibility/Attribution
16-9	User lockout after multiple failed attempts	5%	Quick Win
17-13	Block known file transfer sites	5%	Advanced
5-5	Mail attachment filtering	5%	Quick Win
11-1	Limiting ports and services	2%	Quick Win
13-10	Segregation of networks	2%	Configuration/Hygiene
16-8	Password complexity	2%	Visibility/Attribution
3-3	Restrict ability to download software	2%	Quick Win
5-1	Anti-virus	2%	Quick Win
6-8	Vet security process of vendor	2%	Configuration/Hygiene

<https://www.sans.org/critical-security-controls/controls>



Questions ?



Verizon Data Breach Investigations Report

is available for free download at:

www.VerizonEnterprise.com/DBIR

Bhavesh Chauhan
Principal, Security Engineering
bhavesh.chauhan@verizon.com



Virginia Information Technologies Agency

Upcoming Events





Future ISOAG

September 2, 1:00 - 4:00 pm @ CESC
Speaker: Eric Cowperthwaite, Core Security
&
Karen McDowell, UVA

ISOAG meets the 1st Wednesday of each month in 2015



IS Orientation

When: Thursday, September 24, 2015

Time: 1:00 pm to 3:00 pm

Where: CESC , Room 1211

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



Announcement: VASCAN Conference 2015



They Will Get In. What Are We Doing About It?

Date: October 1-2, 2015

Location: UVA, Newcomb Hall Ballroom

Topics:

- information security
- advanced defense techniques
- IT risk management
- IT regulatory compliance

Bonus Content:

SANS: *Incident Response Management*
MGT535

Meals

- Breakfast and lunch both days
Conference reception Thursday evening,
October 1

To Register: <http://www.virginia.edu/vascan2015/>

ADJOURN

THANK YOU FOR ATTENDING

