CYBERSECURITY:

Mitigating Risks through an Effective IT Audit and Control Program

Virginia Association of School Business Officials
May 24, 2018
Clarence Rhudy, CPA, CISA, CITP

BROWNEDWARDS
certified public accountants

Course Objectives

- Current Cybersecurity Trends and Statistics
- The Role of Audit Committees and Internal Audit
- Understanding Your IT Risks
- Control Frameworks
- Regulatory Considerations
- Vendor Management
- Key Takeaways

Cybersecurity Trends and Statistics:

15 Mindboggling Statistics

1. In 2016, the U.S government spent $28 billion on cybersecurity — and this is expected to increase in 2017-2018
2. According to Microsoft, the potential cost of cybercrime to the global community is $500 billion, and a data breach will cost the average organization about $3.8 million
3. Ransomware attacks increased by 36 percent in 2017
4. The average amount demanded after a ransomware attack is $1,077
5. 1 in 131 emails contain malware

BROWNEDWARDS
certified public accountants

Cybersecurity Trends and Statistics: (cont'd)

15 Mindboggling Statistics

6. In 2017, 6.5 percent of people are victims of identity fraud — resulting in fraudsters defrauding people of about $16 billion
7. 43 percent of cyber attacks are aimed at small organizations
8. Unfilled cybersecurity jobs is expected to reach 3.5 million by 2021 — compared to about 1 million in 2016
9. 230,000 new malware samples are produced every day — and this is predicted to only keep growing
10. 78 percent of people claim to know the risks that come with clicking unknown links in emails and yet still click these links

BROWNEDWARDS
certified public accountants

Cybersecurity Trends and Statistics: (cont'd)

15 Mindboggling Statistics

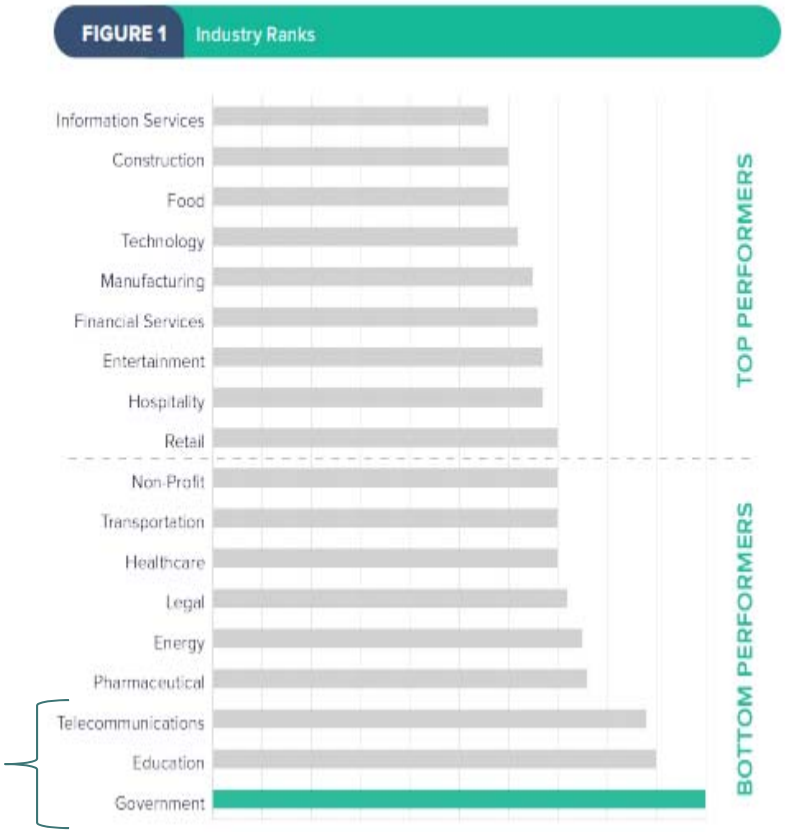
11. 90 percent of hackers cover their tracks by using encryption
12. It takes most businesses about 197 days to detect a breach on their network
13. Android is the second most targeted platform by hackers after Windows
14. 81 percent of data breach victims do not have a system in place to self-detect data breaches
15. 95 percent of Americans are concerned about how companies use their data

BROWNEDWARDS
certified public accountants

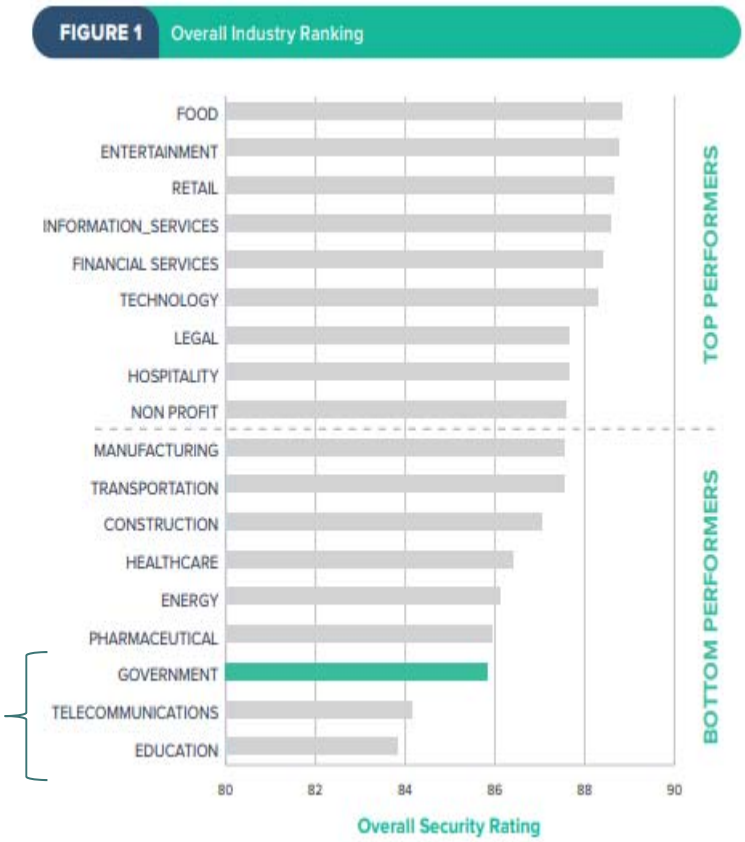
Cybersecurity Trends and Statistics: (cont'd)

Public Sector Industry Trends – SecurityScorecard Report

2016



2017

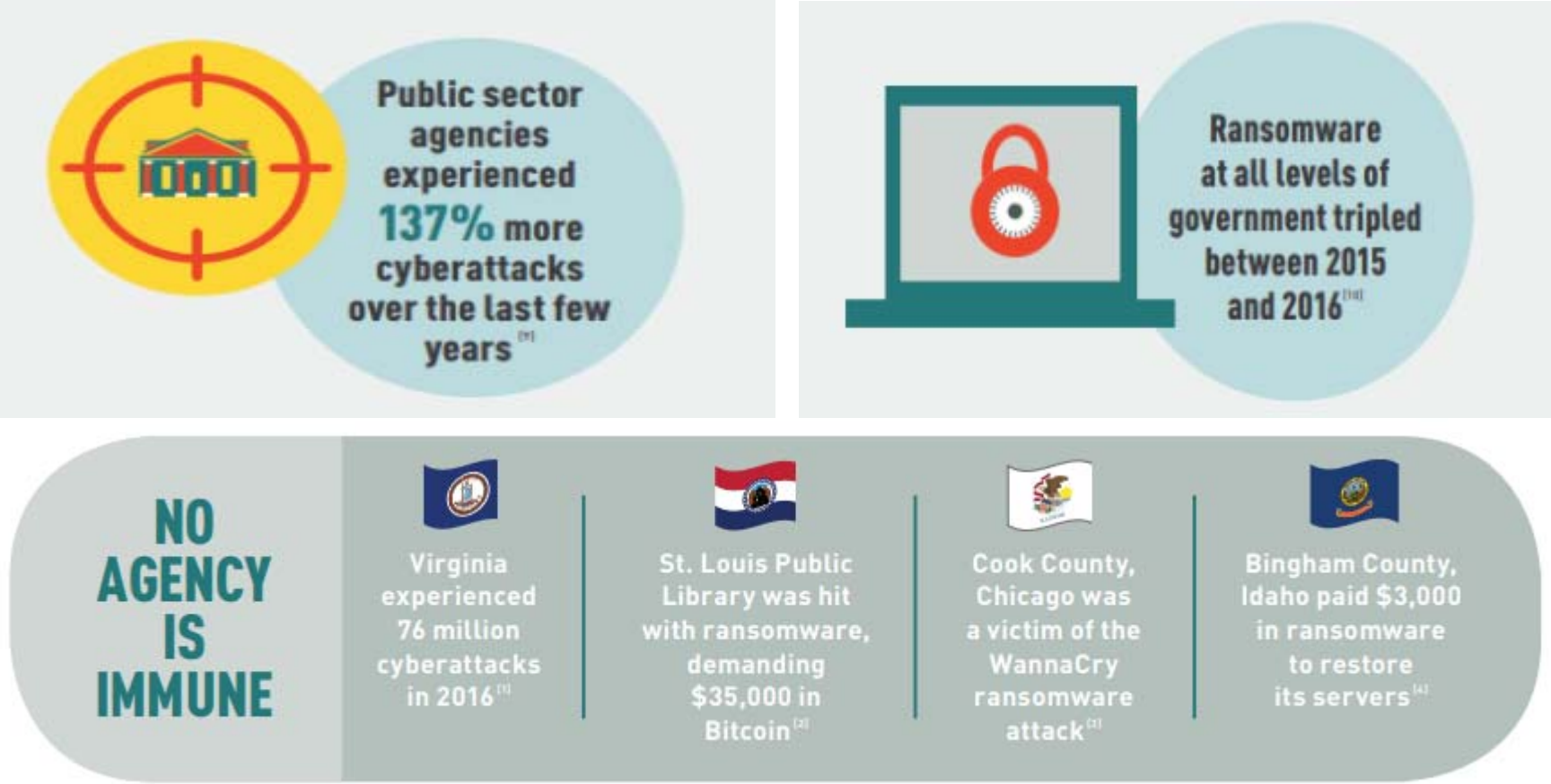


Education and Government Toward the Bottom

BROWNEDWARDS
certified public accountants

Cybersecurity Trends and Statistics: (cont'd)

Public Sector Industry Trends



Cybersecurity Trends and Statistics: (cont'd)

Recent School Data Breaches

Some of the most recent notable reports:

- Florida Virtual School – largest state-run virtual school in the country disclosed in early March 2018 that it had two major data breaches. Records for 368,000 students were left unsecured online for almost two years with no password protection, in addition to a member school district allowing unauthorized individuals to collect social security numbers and other information on up to 50,000 individuals. Children and young adults are a primary identity theft target due to them not having a credit history and virtually unused social security – with parents and children often not checking credit reports for years after such events.

- Pennsylvania State Department of Education – 360,000 notices sent out related to a February 22, 2018 breach. An error by an employee in the Office of Administration opened a windows of 30 minutes where any user logging in could have accessed information in system of any other users which include teachers, school districts and state Department of Education staff. Estimated potential cost of credit monitoring services $641,000.

Cybersecurity Trends and Statistics: (cont'd)

Recent Local Government Breaches

Two major attacks occurred in the space of 3 days during the week of March 19, 2018:

- City of Atlanta – ransomware took much of the city's internal and external services offline. As of March 30, 2018, the city was still attempting to recover from the attack. It is believed that the attack either leveraged open source Java vulnerabilities or applied brute-force password cracking methods to introduce the ransomware.
- Baltimore, MD 911 system – taken offline by a ransomware attack but service restored shortly thereafter. The exploited vulnerability was created due to a firewall change made by a technician troubleshooting the CAD system.

Audit Committees and Internal Audit

Effective risk management is the product of layers of risk defense:

- **Management** –has ownership, responsibility, and accountability for assessing, controlling, and mitigating risks.
- **Risk Management and Compliance Functions** – facilitate and monitor the implementation of effective risk management practices by management, and help risk owners in reporting adequate risk-related information up and down the firm.
- **Internal Audit** – provides objective assurance to the board on how effectively the organization assesses and manages its risks, including the manner in which the first and second lines of defense operate.

Audit Committees and Internal Audit (cont'd)

Audit Committee

Why establish an audit committee?

- **Improve accountability.** Audit committees in the public sector enhance accountability and assist local legislatures in fulfilling their governance responsibilities.
- **Follow best practices.** Audit committees ensure the quality of annual audits and ensure management implements audit recommendations.
- **Ensure Independence.** Audit committees ensure that audit functions are empowered to report issues to oversight authorities.

Audit Committees and Internal Audit (cont'd)

Audit Committee

Are audit committees required?

- **Audit committees are required in some states and localities.** Audit committees for local governments are sometimes required by state or local law. The Government Finance Officer Association (GFOA) recommends that all state and local governments formally establish audit committees by charter or other legal means. Recommendations are similar for other types of organizations

Audit Committees and Internal Audit (cont'd)

Audit Committee

What are the audit committee's responsibilities?

Specific responsibilities vary depending on the form of the orgnaization and reporting relationship to the auditor.

- **Support and oversight of the audit function** – recruiting, appointing, overseeing, and removing (if needed) the auditor; recommendations for the annual audit plan and auditor's budget; ensure independence from management.
- **Oversight of contracts with accounting firms**

Audit Committees and Internal Audit (cont'd)

Audit Committee

How should the audit committee be structured?

- Members should be independent of management
- Members should be collectively knowledgeable about financial matters and the organization
- The audit committee should have the authority and resources to seek outside expertise when necessary
- Stagger terms to ensure continuity

BROWNEDWARDS
certified public accountants

Audit Committees and Internal Audit (cont'd)

Audit Committee

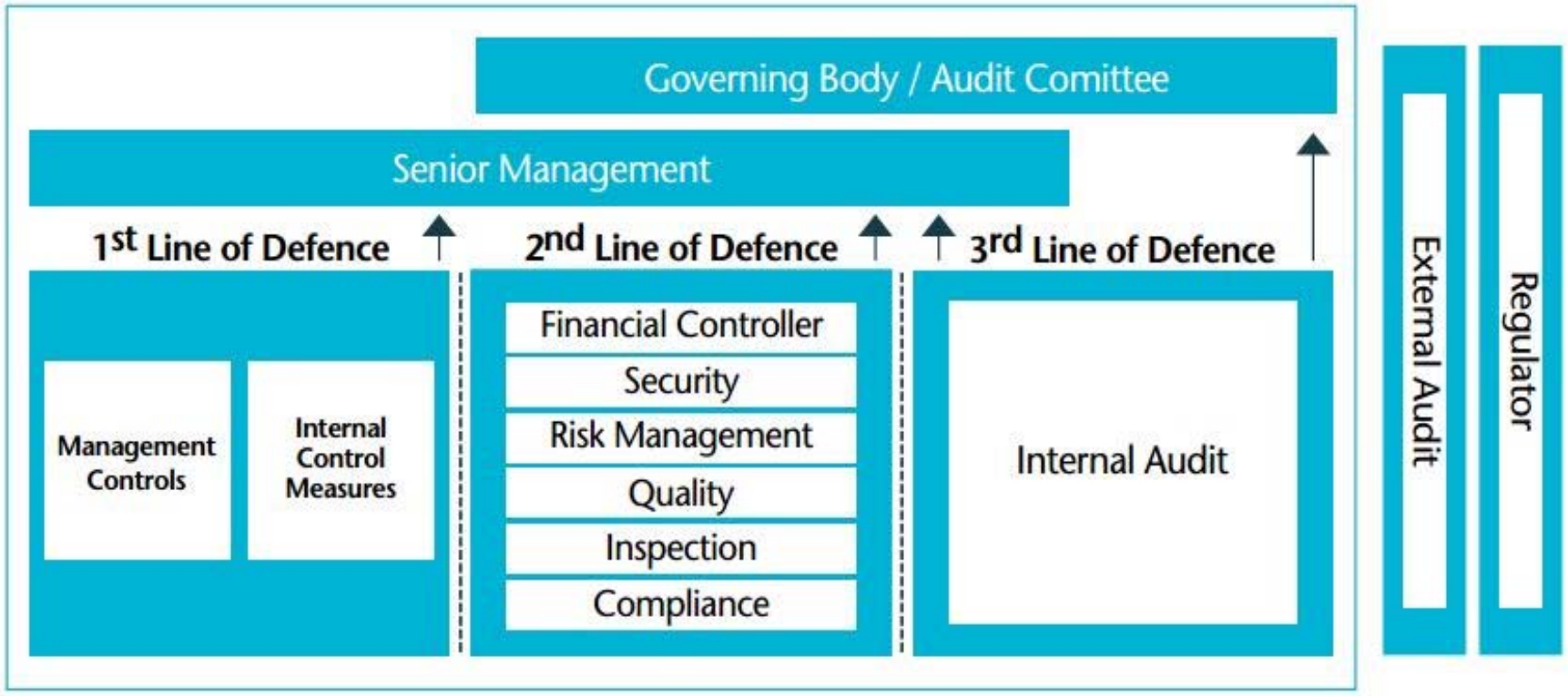
What is an audit committee's (or equivalent) role in cybersecurity?

- Audit committees should be educated on cybersecurity trends, regulatory developments, and major threats to the organization
- Audit committees should have regular dialogue with IT management to better understand where cybersecurity efforts should be focused
- Audit committees should help develop and monitor a cybersecurity plan

Audit Committees and Internal Audit (cont'd)

Internal Audit

The Three Lines of Defense Model



BROWNEDWARDS
certified public accountants

Audit Committees and Internal Audit (cont'd)

Internal Audit

What steps can internal audit take to assist with cybersecurity?

1. Work with management and the BOD to develop a cybersecurity strategy and policy
2. Identify opportunities to improve the organization's ability to identify, assess, and mitigate cybersecurity risk to an acceptable level
3. Assess and mitigate potential threats that could result from actions of an employee or business partner
4. Leverage relationships with the audit committee and board to heighten awareness and knowledge on cyber threats and changing cybersecurity risk
5. Ensure that cybersecurity risk is integrated into the audit plan

Audit Committees and Internal Audit (cont'd)

Internal Audit

What steps can internal audit take to assist with cybersecurity?

6. Develop and maintain an understanding of how emerging technologies and trends are affecting the cybersecurity risk profile
7. Evaluate the cybersecurity program against an agreed upon control framework (such as NIST Cybersecurity)
8. Seek out opportunities to communicate to management that the strongest preventive capability requires a combination of human and technology security
9. Emphasize that cybersecurity monitoring and incident response should be a top priority
10. Identify any IT/audit staffing and resource shortages as well as a lack of supporting technology tools

Understanding Your IT Risks

It is not realistic to perform a risk assessment on every application, function, or process within an organization. Therefore, the first priority should be defining an operational framework by identifying internal and external systems that are critical to your operations or that process, store, and transmit legally protected or sensitive data. Then a risk assessment schedule can be created based on criticality and data sensitivity.

Understanding Your IT Risks (cont'd)

Risk Categories

When going through the process, keep in mind the different categories of risk that may affect your organization:

- Strategic – related to adverse business decisions
- Reputational – related to negative public opinion
- Operational – related to loss resulting from inadequate or failed internal processes, people, and systems, or from external events
- Transactional – related to problems with service or delivery
- Compliance – related to violations of laws, rules, or regulations, or from noncompliance with internal policies and procedures

Understanding Your IT Risks (cont'd)

Basic steps of a risk assessment

1. Characterize the system (process, function, or application) – will help determine the viable threats
2. Identify threats – basic threats will apply to every risk assessment but, depending on the system, additional threats could be included
3. Determine inherent risk and impact – the step is performed without considering your control environment

Understanding Your IT Risks (cont'd)

Basic steps of a risk assessment

4. Analyze the control environment – identify threat prevention, mitigation, detection, or compensating controls in relation to identified threats
5. Determine a likelihood rating – the likelihood of a given exploit taking into account the control environment
6. Calculate your risk rating – impact * likelihood = risk rating

BROWNEDWARDS
certified public accountants

Control Frameworks

A framework is a comprehensive set of practices for implementing security controls to help lower security risks.

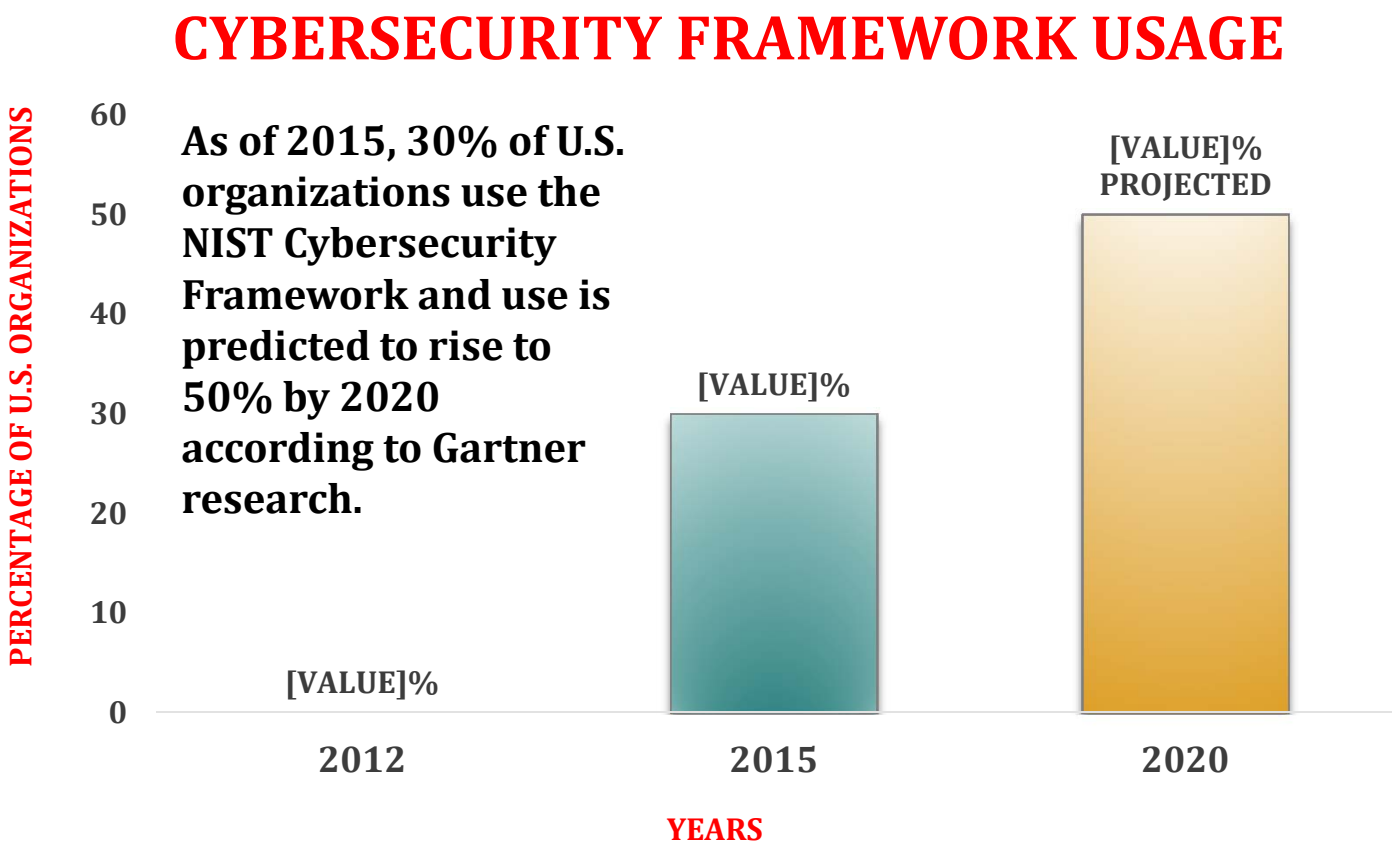
- **International Standards Organization (ISO) 27001** – specifies requirements for an overall management and control framework for managing an organization's information security risks.
- **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53** – provides a catalog of customized security controls and is commonly used by government agencies as their baseline security control framework.

BROWNEDWARDS
certified public accountants

Control Frameworks (cont'd)

- **NIST Cybersecurity Framework (CSF)** – helps owners and operators of critical infrastructure to manage cybersecurity-related risk.
- **Federal Information Processing Standards (FIPS)** – publicly announced standards developed by the U.S. government for use in computer systems by non-military agencies and government contractors.

Control Frameworks (cont'd)



Control Frameworks (cont'd)

Security Reference Material

The references listed below provide additional guidance for various cybersecurity topics that are addressed in the various control frameworks.

- **ISO 27002** – related to ISO 27001
- **NIST SP 800-44** – public web servers
- **NIST SP 800-45** – mail servers
- **NIST SP 800-50 and SP 800-16** – IT security training program
- **NIST SP 800-66** – The Health Insurance Portability and Accountability Act (HIPAA) Security Rule concepts

Control Frameworks (cont'd)

Security Reference Material

- **NIST SP 800-123** – network communication servers
- **NIST SP 800-124** – mobile devices
- **NIST SP 800-125** – virtualization technologies
- **NIST SP 800-144** – cloud computing
- **NIST SP 800-153** – wireless networks
- **Federal Information Processing Standards (FIPS) 200** – security requirements for federal information systems
- **FIPS 140-1 & 2** – cryptography modules

Regulatory Considerations

An organization may have to comply with many regulations such as:

- FERPA
- HIPAA
- The Health Information Technology for Economic and Clinical Health Act (HITECH)
- CMS Information Security Acceptable Risk Safeguards (ARS)
- 42 Code of Federal Regulations (CFR)
- Criminal Justice Information Services (CJIS) Security Policy
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Information Security Management Act (FISMA)

Regulatory Considerations (cont'd)

Relevant Virginia State Laws

At least 42 states have introduced more than 240 bills or resolutions related to cybersecurity. Listed below are a few Virginia state laws that address information security:

- Va. Code § 2.2 – 603: Every agency and department is responsible for securing electronic data and shall comply with the requirements of the commonwealth's information technology security and risk-management program as set forth in Va. Code § 2.2-2009, and shall report all known incidents that threaten data security.
- Va. Code § 2.2 – 2009: The CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information.
- Va. Code § 18.2-186.6 and § 32.1-127.1:05: Breach disclosure statutes

* Disclaimer: I am not a lawyer. Please check with legal counsel to understand current laws and regulations and to determine your organization's specific compliance requirements.

Regulatory Considerations (cont'd)

Vigilance is Imperative

Keeping up to date with regulations is important but does not guarantee organizations are secure. True security depends on minimizing IT risks rather than checking all the right boxes. Leaders shouldn't let satisfactory compliance reports lull them into complacency. Be prepared for today's and tomorrow's hackers, not yesterday's!!

A proactive approach includes:

- Conducting periodic security assessments
- Evaluating incident response readiness
- Leveraging an effective control framework

Vendor Management

More and more, organizations are asking third parties to become involved in managing and operating the organization's technology. Benefits to outsourcing IT may include:

- Controlling and reducing the rising costs of IT
- Achieving greater efficiency
- Making technology solutions more responsive to change

Any vendor who has access to your data or who has access to your internal network is a potential risk that must be closely monitored.

BROWNEDWARDS
certified public accountants

Vendor Management (cont'd)

What's in a vendor management program?

A vendor management program consists of 4 basic steps:

1. Identify and rank your vendor list – it's important to identify all vendors that have access to sensitive data as well as your network. In addition, vendors should be ranked according to the risk associated with the relationship.
2. Perform due diligence – research the vendor to determine their cybersecurity capabilities. Further, contract language should be developed that requires the behaviors and controls you deem necessary.

Vendor Management (cont'd)

What's in a vendor management program?

A vendor management program consists of 4 basic steps:

3. DOCUMENT!! – the results of the due diligence need to be documented. Create a spreadsheet or database to track all vendors and their ongoing review schedules.
4. Report – You should have a mechanism to report serious issues to senior management and be prepared to demonstrate the results of your vendor management program to auditors. It is recommended that critical and high risk vendors be reviewed at least annually.

The vendor management process is
not a one and done exercise

Key Takeaways

- It is not possible to eliminate all risk
- Create appropriate risk assessments for Cybersecurity
- Create and communicate an information security policy and records management process
- Leverage existing control frameworks to develop and implement information security internal controls
- Create and deliver information security training
  - Human negligence is often the biggest risk to organizations
  - Many attacks could have been avoided if users had installed months-old security patches
- Hire experienced, qualified, and certified IT professionals
  - CISA, CISSP

Key Takeaways (cont'd)

- Develop an incident/breach response process
  - Developing a plan that details breach notification protocols and identifies the critical stakeholders involved in containing, removing, and communicating the threat can ensure the organization's response is immediate and comprehensive
- Create and implement an information assurance business continuity plan
- Select and implement appropriate and affordable information security tools and technologies
  - Threat monitoring and analytical tools are critical weapons in an organization's defense arsenal

Key Takeaways (cont'd)

- Create and communicate a security patch management program
  - Keeping operating systems and software updated with the latest security patches can reduce the number of exploitable entry points. Organizations must develop a solid understanding of the vulnerabilities that exist and the degree of risk they present to ensure the appropriate measures are taken to address them.

Key Takeaways (cont'd)

Conduct periodic cybersecurity assessments both internally and via independent consultations

- Examples of internal audit focus areas
  - IT governance
  - Change management
  - Logical and physical access
  - Mobile computing
  - Penetration testing
  - Vulnerability management
  - Business continuity planning
  - Crisis management
  - Vendor management
- Examples of independent assessments
  - FedRAMP Third Party Assessor Organization Cloud Security Assessment Reports
  - FISMA Security Assessments
  - IT Internal Audit Co-sourcing/Outsourcing
  - SOC Reports
  - Vulnerability/Penetration testing

Clarence Rhudy, CPA, CISA, CITP
crhudy@becpas.com
540 345-0936

BROWNEDWARDS
certified public accountants