2021 Summer CPE Series:

Manage and Defend Against Cybersecurity Risks

Michelle Chopper

Chris Ferguson

Steve Guarini

Cohen & Co®

Presenters:

Steve Guarini, CPA
Partner, Cohen & Company
sguarini@cohencpa.com
586-541-7736

Michelle Chopper, CPA
Director, Cohen & Company
michelle.chopper@cohencpa.com
410-527-3972

Chris Ferguson, CPA
Manager, Cohen & Company
christopher.ferguson@cohencpa.com
410-891-0378

Learning Objectives

- Understand cybersecurity principles and key risks and controls
- Identify types of attacks and key cybersecurity threats
- Introduction of the five cybersecurity functions and their purpose
- Understand the cybersecurity frameworks
- Navigate the processes and controls needed to detect, respond to, mitigate and recover from a security incident

Cohen & Co®

Why care about cybersecurity?

- Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

Costs of data breach expected to grow 15% over the next 5 years.

- 2021 Report: Cyber Warfare in the C-Suite published by Cybersecurity Ventures

The average cost of a data breach in the U.S. is nearly $8.6 million.

- IBM Cost of a Data Breach Report 2020

Potential to reach $10.5 trillion by 2025 – greatest transfer of economic wealth in history

- 2021 Report: Cyber Warfare in the C-Suite published by Cybersecurity Ventures

What is cybersecurity?

- Process of designing, implementing, and operating controls and other risk management activities to:
  - Protect information and systems
  - Detect, respond to, mitigate, and recover
- Cybersecurity programs can help identify, manage, and communicate security risks

The objective of an information security program is to identify, catalog, measure and manage security risks to an acceptable level.

The three tenets of information security

- Confidentiality
  - Data is kept private
- Integrity
  - Data can be trusted
- Availability
  - Data can be accessed when needed

Types of sensitive data that should be protected

Personally identifiable information (“PII”)	Protected health information (“PHI”)	Cardholder data	Proprietary information
• Social Security Number, Drivers License Number, account numbers, addresses, etc.	• Health details on a person, such as a malady that can be tied to an individual	• Credit card data	• Trade secrets or competitive intelligence

Polling Question #1

- What are the three tenets of information security? (Select all that apply)
  A. Data is kept private
  B. Information security is only relevant to IT professionals
  C. Data can be trusted
  D. Information should always be publicly available
  E. Data can be accessed when needed

Why do attackers attack?

- Attackers may have many different motivations for attacking an organization, including:
  - Sell sensitive data for profit (black market / dark web)
  - Identity theft
  - False tax return filings
  - Intellectual property theft
  - Healthcare fraud
  - Political / social convictions
  - Nation state attacks

Key cybersecurity terms

- **Risk Assessment** – process of identifying, measuring, and communicating security risks in an organization
- **Risk** – likelihood there will be a successful exploit of a vulnerability
- **Exploit** – attack that takes advantage of a vulnerability
- **Vulnerability** – weakness that could allow an attacker to compromise confidentiality, integrity, or availability
- **Cost** – the balance of how much does it cost to protect the information vs cost if information is lost

An overview of key cybersecurity risks

- Cyber Risks are Constantly Evolving
  - Attackers get more sophisticated and find new ways of breaking into systems.
  - Availability of easy-to-use tools reduce the level of skill required to carry out attacks.
  - Vulnerabilities change as businesses change.
- Cyber Risks are Broad and Connected
  - Cyber risks are multifaceted in nature and require a variety of different measures across the organization.
  - The impact of failures cannot necessarily be contained within single systems, networks or organizations, creating potential systemic risks.

Common Cybersecurity Attack Techniques

Malicious software or ransomware, downloaded to a target computer	Phishing emails crafted to trick victims into giving up passwords and other credentials or taking some other malicious action
Denial of Service (DoS) attacks, which overwhelm a server, system or network with bogus traffic	Man in the middle attacks, which fool the target computer into joining a compromised network

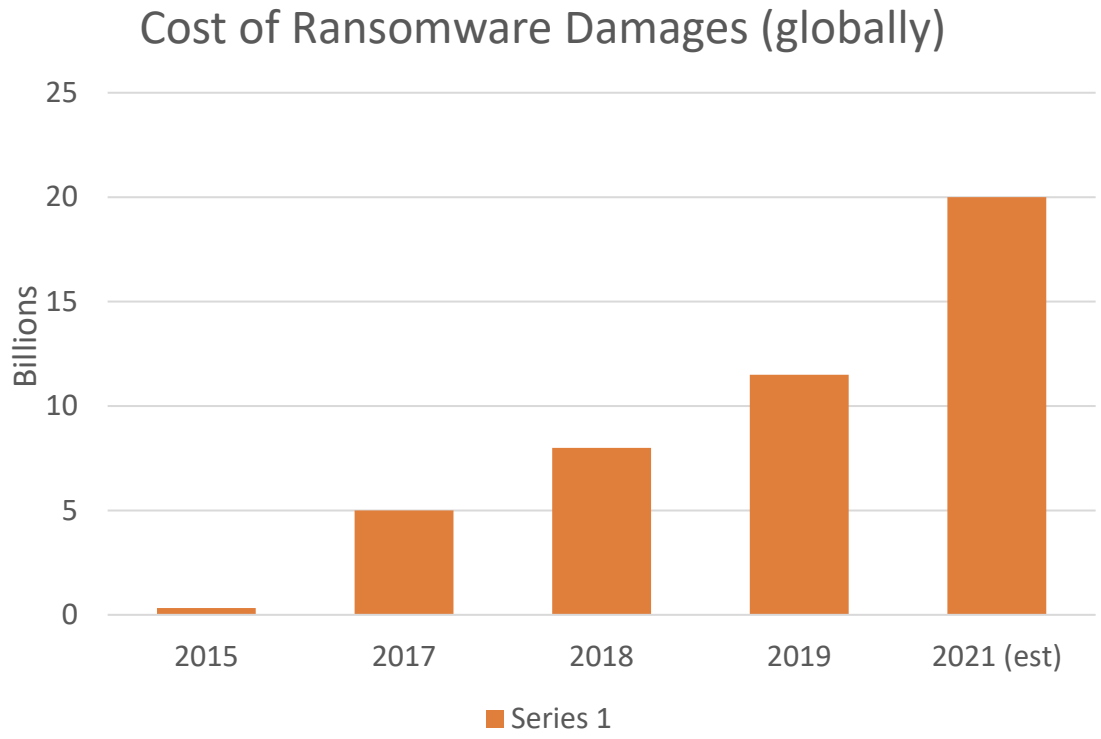
Techniques may be used in tandem. e.g., attacker uses phishing emails to trick users into downloading malware

Cohen & Co

Examples of key cybersecurity risks & controls

Vulnerabilities exploited to gain access to sensitive information due to unpatched or unsupported IT systems	Vulnerabilities exploited to gain access to sensitive information due to poorly configured IT systems	Ransomware or other malicious attacks due to failure to continuously monitor for, and defend against, malware	Business disruption from phishing or malware attacks due to employees' lack of awareness of cybersecurity threats	Hackers gain access to confidential data through man in the middle or other means of attack
• Routinely patch servers, and desktop/laptop systems • Ensure infrastructure systems and applications are currently supported by vendors • Routine vulnerability scans to identify system vulnerabilities	• Ensure system hardening through baseline configuration standards • Routinely review hardening guidelines • Implement Automated Configuration Monitoring Systems	• Implement centrally managed anti-malware tool • Provide Ongoing security awareness training • Use Domain Name System (DNS) filtering services to help block access to known malicious domains.	• Provide Ongoing security awareness training • Implement and routinely test an incident response plan	• Encrypt confidential data at rest and during transfer • Identify and classify data according to risk and restrict accordingly • Security awareness training

Cybersecurity enemy #1… Ransomware



A malware that infects computers (and mobile devices) and restricts their access to files, often threatening permanent data destruction unless a ransom is paid

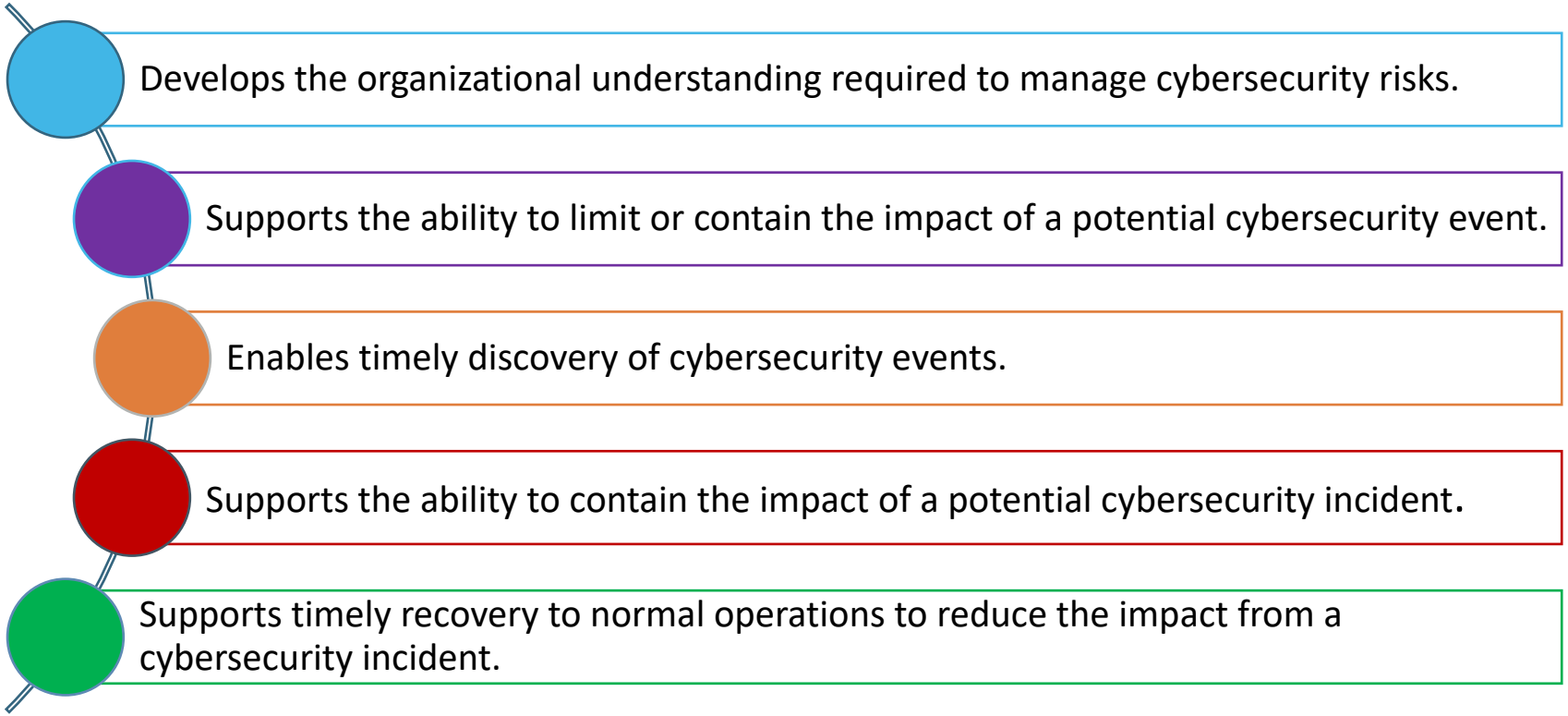
Polling Question #2

- Which of the following increases exposure to cybersecurity risks (select all that apply)
  A. The organization does not currently have a security awareness training program for employees
  B. The IT organization implemented new application functionality without performing User Acceptance Testing
  C. Several systems are running Windows Server 2003 which is no longer supported by the vendor
  D. The organization currently does not patch end user laptops and desktop systems
  E. A key application was accidentally configured with incorrect threshold for Journal Entry approval

The five cybersecurity functions

Overview of the five cybersecurity functions

- The security functions organize basic cybersecurity activities at their highest level.
- They aid organizations in expressing their management of cybersecurity risk at a high level.



Examples of the Five Cybersecurity Functions

Identify	Protect	Detect	Respond	Recover
- Identifying physical and software assets within the organization - Identifying legal and regulatory requirements regarding the cybersecurity capabilities - Identifying asset vulnerabilities, threats to organizational resources, and risk response activities	- Protections for Identity Management and Access Control including physical and remote access - Empowering staff within the organization through Awareness and Training - Establishing Data Security to protect the confidentiality, integrity, and availability of information	- Detecting anomalies and events and evaluating their potential impact - Implementing Security Continuous Monitoring capabilities to monitor cybersecurity events - Maintaining Detection Processes to provide awareness of anomalous events	- Ensuring Response Planning process are executed during and after an incident - Managing Communications during and after an event with stakeholders, law enforcement, etc. - Conducting analysis to ensure effective response and support recovery activities including forensic analysis, and determining the impact of incidents	- Implementing Recovery Planning processes and procedures to restore systems and/or assets affected by cybersecurity incidents - Implementing Improvements based on lessons learned and reviews of existing strategies - Internal and external Communications are coordinated during and following the recovery from a cybersecurity incident

Polling Question #3

- Which of the security functions supports the organization's ability to limit (or contain) the impact of a potential cybersecurity event?
  A. Identify
  B. Protect
  C. Detect
  D. Respond
  E. Recover

Cybersecurity Frameworks

Cohen & Co

Cybersecurity Frameworks

Framework	Use Case(s)	Overview
NIST Cyber Security Framework	- Cybersecurity program maturity assessment - Cybersecurity risk assessment - Cybersecurity controls assessment	- Focused on the overall program level, this framework offers implementation tiers to assist organizations in establishing their cyber risk management approach - Methodology facilitates developing current and target state cybersecurity profiles and defining steps to achieve target state
ISO 27000	- Information security management systems	- Focused on three main areas of a mature cybersecurity management program: people, processes and technology - Includes greater security standards and protections including physical and operational security measures and broken down into Series to get more specific into implementation and design of the model
CIS 20 (Center for Internet Security)	- Cybersecurity controls assessment	- Controls level framework consists of critical security controls for mitigating cybersecurity risks. - Separates controls across three implementation groups determined by organization's size and availability of IT expertise among other factors.
HIPAA / GDPR / Other	- Industry specific secondary frameworks	- HIPAA was created to require healthcare organizations to protect the privacy and highly sensitive information of patients. Extends to other organizations with employee healthcare information. - GDPR focuses on the requirements of organizations in the EU to protect consumer data & includes data protection for info transferred from EU-based organizations to somewhere else geographically.
Cybersecurity Risk Management Reporting Framework (SOC For Cyber)	- Cybersecurity program maturity assessment	- Program level framework to support developing and assessment of cybersecurity risk management program. - Facilitates formal documentation of the description of the entity's cybersecurity risk management program including the controls within that program to achieve the entity's cybersecurity objectives.

Cybersecurity Considerations

- Misstated Financials Resulting From Cyber Related Data Integrity Risks
  - An organization typically designs and implements cybersecurity controls to protect the integrity, confidentiality, and availability of information.
  - Traditionally, the financial auditor relies on the testing of IT General Controls to address IT risks
  - Cyber criminals can exploit vulnerabilities to **bypass IT General Controls** and secure access to modify IT applications and (financial) data.
  - Cyber criminals will cover their tracks to avoid being detected by audit logging & monitoring activities.

Case Study

A manufacturing company was subject to an unidentified cyber-attack, which deleted some of its financial reporting data.

Failing to identify the attack or not having adequate data backup and recovery controls may cause the company to present inaccurate or incomplete financials.

Cybersecurity Considerations

- Misstated Financials Resulting From Failure to Identify and Understand the Impact of Cybersecurity Incidents
  - Cyber incidents can result in significant financial consequences and may ultimately have an effect on financial statements
  - The financial impact on businesses can cause fundamental enterprise-wide damage
  - Cyber attacks may go undetected, resulting in financial implications to the entity that may not be reflected in the financial statements

Financial Impacts of Cybersecurity Incidents

- Loss of customers and revenue
- Significant unexpected costs related to lawsuits and settlements
- Regulatory penalties for breaching data privacy legislation.
- Lost revenue due to extended downtime and cease of business operations.

Case Study

A technology company experienced a cyber-attack which resulted in the theft of its patented new technology that is recognized as an intangible asset for a material amount.

The theft resulted in an undetected impairment issue that may impact future earnings and cash flows.

Cybersecurity Considerations

- Cyber Related **Disclosure** Considerations
  - On October 13, 2011, the SEC issued a CF Disclosure Guidance requiring **publicly traded companies** disclose cyber-attacks to regulators and explain the measures they plan to take to close their cyber-security gaps.
  - The Guidance provides that if one or more cyber incidents materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions, the company should provide disclosure.
  - The Guidance states that public companies should disclose the risk of cyber incidents if they are "among the most significant factors that make an investment in the company speculative or risky".

Uber paid the perpetrator of its 2018 data breach $100,000 to keep the breach secret resulting in a $148 million fine for violation of state data breach notification laws.

In 2019, the SEC announced a $100 million settlement with Facebook, arising from alleged misstatements in its disclosure.

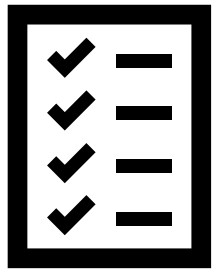
In 2013, Yahoo failed to disclose it suffered a security breach that affected about 3 billion accounts. The SEC fined the company $35 million for failing to disclose the breach.

Cybersecurity vs IT General Controls (ITGCs)

- IT General Controls
  - Aims to protect information from theft, misuse, unauthorized access, and modification
  - Ensures the quality, confidentiality, and accessibility of data when needed
  - Broad scope includes steps that also protect your data across the internet
  - Cover all data created or collected by the company. This protection will include (and extend beyond) the internet
  - IT security also covers physical data, in-house systems, and other channels that don't include the cybersecurity space
- Cybersecurity Controls
  - Aims to protect company data from threats that may occur on the internet
  - Cybersecurity protects electronic data that's being transmitted across the internet or stored on systems accessible via the internet

Cybersecurity vs IT General *Processes*

- Cybersecurity Controls Processes (non-exhaustive)
  - IT Asset Management
  - Vulnerability Management
  - Configuration Management
  - Network Security
  - Data Security
  - Malware Defenses
  - Security Awareness Program
  - Incident Response
- IT General Controls Processes
  - Change Management
  - Logical & Physical Security
  - System Development Life Cycle
  - Computer Operations



Polling Question #4

- ITGCs are **not** sufficient to mitigate cybersecurity risks because:
  A. Vulnerabilities may be exploited allowing a hacker to bypass IT General Controls
  B. ITGCs are generally not well designed
  C. ITGCs do not address application specific risks
  D. ITGCs sufficiently mitigate cybersecurity risks

Cohen & Co®

Reduce your exposure – do this today!

Employ tools to automatically identify potential problems

- Vulnerabilities such as unpatched systems, open ports, misconfigured software, etc can be hidden – you need tools that can automatically and proactively identify areas of cyber exposure to tackle them intelligently and with a focused effort

Create a cyber exposure response team

- Preparing for and responding to cyber threats is not the job of one person or just the IT dept
- IT and CISO likely manage the immediate threat
- Legal involved in the event of data exposure
- Communications team & sales team must be prepared with a communication plan
- HR managers may need to work through employee concerns and step in if employee information was compromised

Have a plan in place to alert stakeholders in case of a breach

- Customers and partners should have the following explained: what happened, how it impacts them, what you're doing to address it now and in the future
- Vendors or other third parties you interconnect with should also have the appropriate information to assess if their networks have been impacted

Continuously monitor to prevent the next threat

- We recommend continuous monitoring of both your and your third-party vendors attack surface
- Annual or bi-annual questionnaires and assessments start with establishment of the baseline security posture and may assist in developing target state goals
- Also need routine monitoring of user behavior, insights into vendors' patching cadence.

Reduce your exposure - remember your vendors!

- Hold your vendors accountable to a cybersecurity baseline
  - Several are available and explicitly designed for third-party risk management (Examples: NIST Framework for Improving Critical Infrastructure Cybersecurity, the SANS Top 20 Critical Security Controls, and Shared Assessments)
- Effectively measure security performance using a tiered approach to assess your vendors according to their criticality to your business and the inherent risk you're willing to accept
- Consider continuous monitoring tools for critical vendors for real-time alerts and security management

Questions?

Steve Guarini, CPA
Partner, Cohen & Company
sguarini@cohencpa.com
586-541-7736

Michelle Chopper, CPA
Director, Cohen & Company
michelle.chopper@cohencpa.com
410-527-3972

Chris Ferguson, CPA
Manager, Cohen & Company
christopher.ferguson@cohencpa.com
410-891-0378