June 22, 2022 | 11:00 A.M. ET

rkl

WHAT'S NEXT ›

WEBINAR SERIES

Insights & education on the latest issues impacting people, profits and processes

Housekeeping Items

- The webinar will be recorded and shared as soon as it is available via email
- Today's materials will be shared in the chat box
- All lines are muted
- NASBA CPE requirements – in order to receive CPE for this webinar:
  - Participants must be connected to the session (both audio and presentation) for its entirety
  - Participants must answer three questions/elements of engagement
  - One (1) hour of CPE in the field of information technology will be granted if you meet these requirements

DISCLAIMER: The presenters, Michael McAllister and James Ruffin and RKL LLP and its subsidiaries/affiliates are not held responsible for information that has changed or will change and makes no representation or warranty as to the ongoing accuracy of the information presented orally or in writing. Attendees should consult with legal, accounting and other advisors.

Welcome and Meet Your Team

Michael McAllister, CPA. CITP, CISA

Partner, IS Assurance and Advisory Services

Michael McAllister serves as the Partner for RKL's IS Assurance and Advisory Services Group, with his focus on supporting the accounting world and helping clients navigate through the issues and concerns that may keep them up at night. With more than 25 years of experience in accounting and information security, Michael builds the knowledge bridge between the financial aspects of accounting, and the information technology systems and controls that support each process. Together with his IS Assurance and Advisory Services team, he serves clients in a variety of industries, ranging from manufacturing to retail, technology and financial institutions; providing information technology internal audits, IT governance reviews, cybersecurity assessments, and compliance evaluations with various IT security standards.

James Ruffin, CPA, CISA

Manager, IS Assurance and Advisory Services

James is a manager in RKL's IS Assurance and Advisory Services Group. He specializes in providing IT Internal Audit services (SOX Readiness / Support, IT Internal Audit, Application / Procedure Assessments) for publically traded banking institutions and Fortune 500 manufacturing companies. James' experience also includes performing SSAE 18 (SOC) attestation services and IT General Controls risk assessment services. Throughout his career, James has served clients in a range of industries, with a concentration in financial institutions, manufacturing & distribution and hospitality. He joined RKL in 2019, bringing with him five years of public accounting experience. In his previous role at a top five national accounting firm, James provided financial statement audits for SEC registrants and non-public companies, before transitioning into IS Assurance services.

What Will We Introduce

01.

Cybersecurity Risks

What are the top 10 cybersecurity threats for 2022 and how could they be affecting your business?

02.

Data Security

Defense in layers is the best way to prevent or limit potential breach consequences.

03.

The "Bump in the Night"

Even with the best laid plans, it is very hard to prevent everything. Having the right plans and procedures in place to react are essential.

04.

Cybersecurity Insurance

A partner in the on-going cyber battlefield, insurance can provide an additional ally should the unthinkable occur.

POLLING QUESTION

To be eligible for CPE, 3 polling questions must be answered.

Cybersecurity Risks

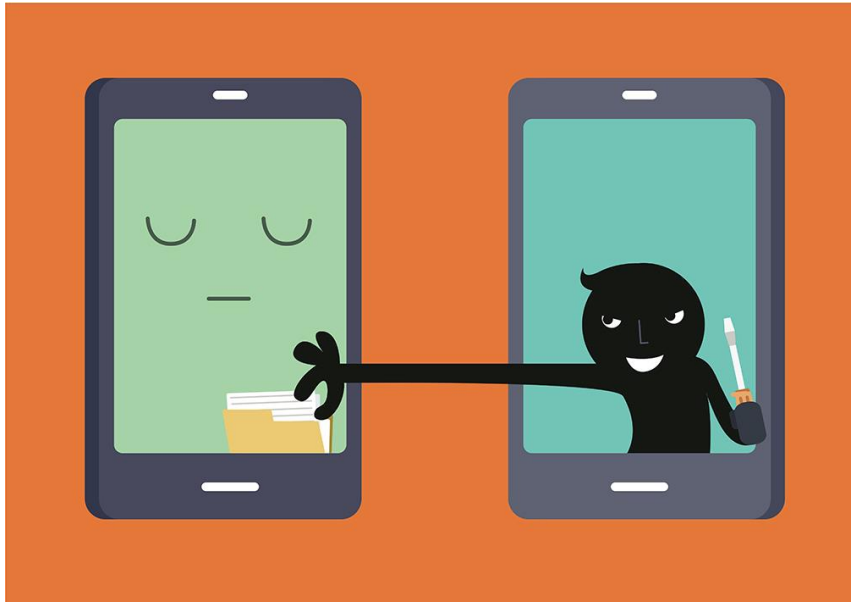
- Top 10 cybersecurity threats identified for 2022

- The more things change, the more they stay the same

Top 10 cybersecurity threats for 2022

- Social engineering
- Third party exposure
- Configuration mistakes
- Poor cyber hygiene
- Cloud vulnerabilities

Top 10 cybersecurity threats for 2022 (continued)



- Mobile device vulnerabilities
- Internet of things
- Ransomware
- Poor data management
- Inadequate post-attack procedures

The more things change, the more they stay the same

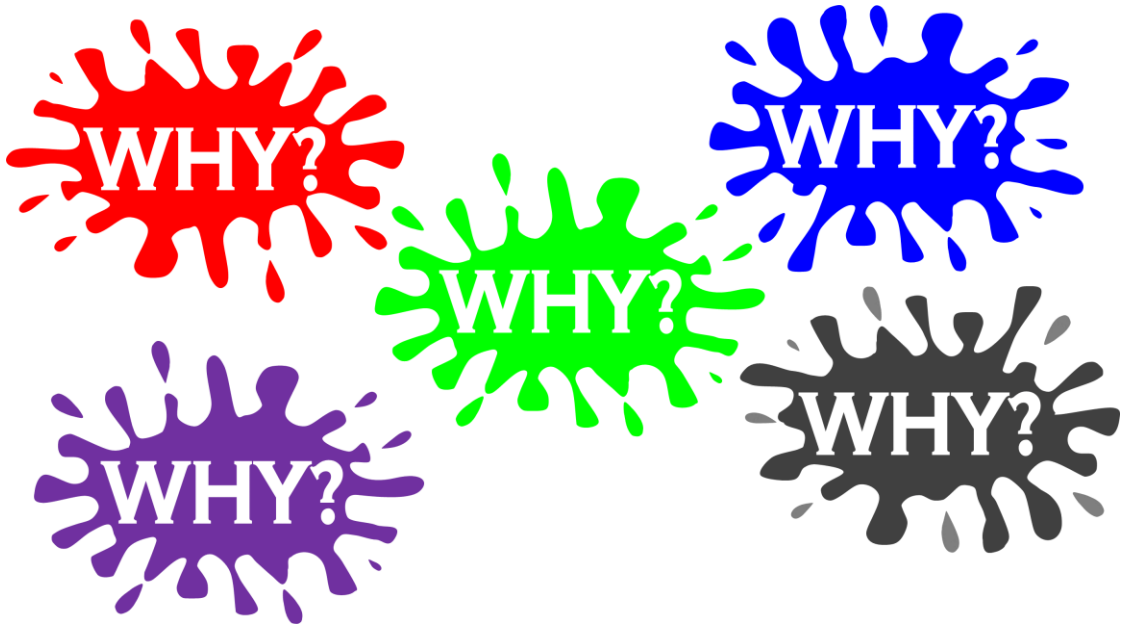
- How different are these from the 2021 or 2020 threats?

- The majority of issues center around the “human element”

Cyber Hygiene – Defense in Layers

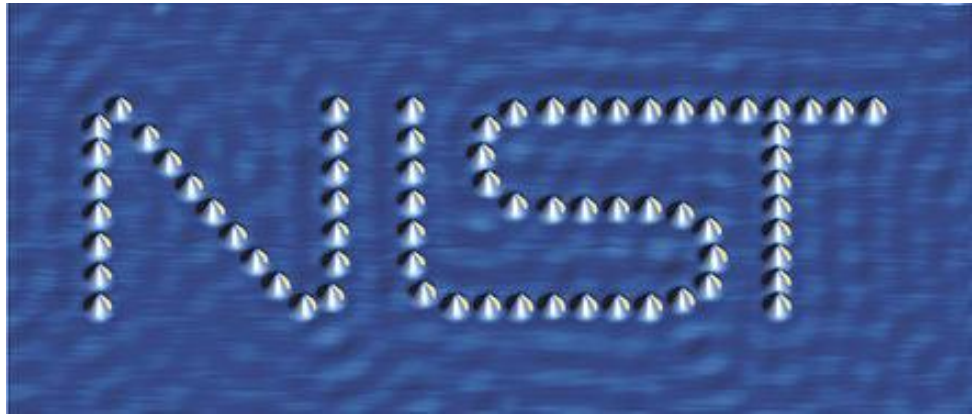
- Frameworks
- Data security
- Infrastructure
- Knowledge
- Vendor management

Frameworks – Why are they important?



- Great starting point for establishing good policies, procedures and operational activities
- Reduces the risk and impact of cybersecurity issues
- How do you choose the right one?

Frameworks - National Institute of Standards and Technology (NIST)



- NIST SP 800-53 – extensive IT standards
- NIST SP 800-171 – Department of Defense, less detailed than 800-53
  - Basis for the new CMMC
- NIST CSF – focuses on risk analysis and risk management

Frameworks - Control Objectives for Information Technology (COBIT)

- Focuses on reducing IT risks
- Is the most used framework to achieve Sarbanes-Oxley compliance
- Distinguishes between risk governance and risk management activities

Frameworks - Having the right framework does not solve all risks

Additional considerations when selecting and implementing any IT security framework:

- Cost benefit / return on investment
- Establishing procedures / controls that are repeatable
- Setting the right expectations

Data Security

- Access management
- Security management
- Change management (software & configurations)

Infrastructure

- Firewalls / monitoring
- Patching
- Data location and encryption

Infrastructure – Data location and encryption

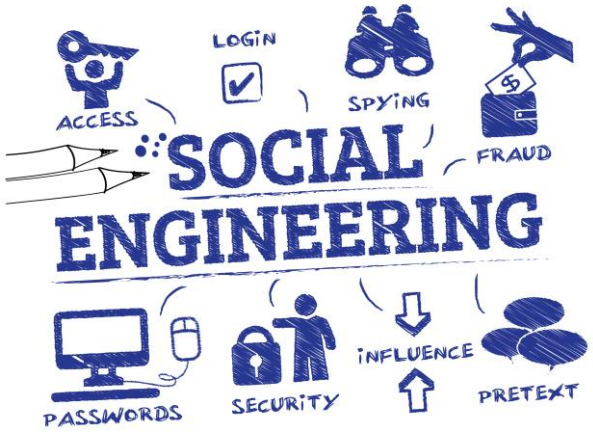
How is the data safeguarded?

- In transit and at rest
- Where is the data stored and is access appropriate for business needs

Knowledge

- Social engineering
- Employee security training
- Data classification

Knowledge – Social Engineering | Focused Attacks



Social engineering threats to watch out for:

- Business email compromise
- Extortion / ransomware
- Pretexting
- Whaling and cat phishing scams

Hackers are getting creative

- Local events
- Scenarios specific to remote employees

Knowledge – Social Engineering | Prevention

- Security awareness training
  - Social engineering exercises
    - Lather, rinse, repeat

- Communicate expectations to employees and if necessary, consequences

Knowledge – Data Classification

Different types of data:

- Public information
- Non-public information (sensitive / confidential)

Disposition of data / retention policy being followed

Vendor Management

- Types of risk associated with outsourcing services
- Board and senior management responsibilities
- Initial / on-going due diligence

POLLING QUESTION

To be eligible for CPE, 3 polling questions must be answered.

Vendor Management - Types of Risks

- Risks related to the function outsourced
  - Sensitivity of data accessed, protected, or controlled
  - Volume of transactions
  - Criticality to the company's business
- Operational or transaction risks
  - Fraud
  - Errors
  - Inability to deliver products or services
- Reputational risks
- Strategic risks
- Compliance risks

Vendor Management - Board and Senior Management Responsibilities

- Risk based policies to govern the outsourcing process (approved by the Board of Directors or sub-committee)
  - Framework (risks)
  - Identify
  - Measure
  - Monitor
  - Control
- Considerations
  - Does the relationship support the company's overall requirements and strategic plans?
  - Is there sufficient expertise to oversee and manage the relationship?

Vendor Management – Initial and On-Going Due Diligence

Considerations:

- Reputation
- Financial strength
- Prior history of security issues
- Availability of reports concerning security / controls around their service

The "Bump in the Night"

- Business Continuity Plan
- Incident Response Plan

Business Continuity Plan

- Business Continuity Plan
- Did the current plan work as expected?
- Did the employees know what to do?
- What were the lessons learned?

Incident Response Plan

Plan of action when a breach has occurred

- What do you do first?
- Who should you contact?
- Do you need to contain (forensic evidence)?

Cybersecurity Insurance

- What is it? Risk transferred
- Covered risks and boundaries
- Understand the requirements and stay compliant

POLLING QUESTION

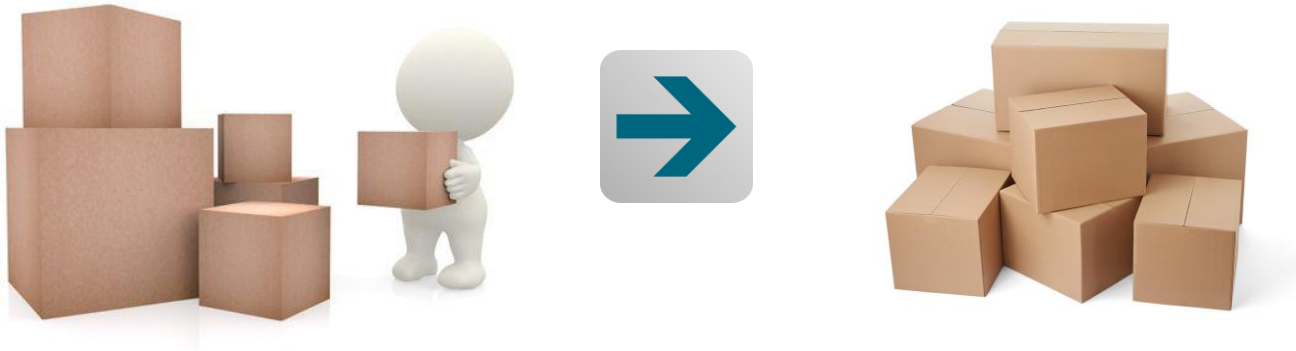
To be eligible for CPE, 3 polling questions must be answered.

Cybersecurity Insurance - What is it? Risk Transferred.

Cover financial costs / liabilities associated with experiencing a cyber security incident.

Incident examples:

- Ransomware
- Network breach
- Compromised users
- Theft of funds or information



Cybersecurity Insurance - Boundaries

Covered Risk	Description
Service	Meeting customer obligations and expectations
Privacy	Sensitivity of data maintained
Operational	Reliance on technology for day-to-day
Security	Breach / Network

What's *not* typically covered

- Act of war
- Future profit (general)
- System *betterment* post incident

Understand the Requirements and Staying Compliant

- As few as eight requirements
- As high as thirty-five requirements
- All providers are different, though some similar trends are present

- Know what is expected
- Meet those expectations
- It is not a 'diet'

POLLING QUESTION

To be eligible for CPE, 3 polling questions must be answered.

Do You Have Questions?

rkl ADVISORS for WHAT'S NEXT

Thank You for Joining Us

Whatever your next move, we're here to help.

Michael McAllister
mmcallister@rklcpa.com

James Ruffin
jruffin@rklcpa.com

- Visit rklcpa.com for more updates and guidance
- Registration open soon: July 20 What's Next Webinar – *Economic Update*