BAKER
NEWMAN
NOYES

2021 Accounting & Business Update

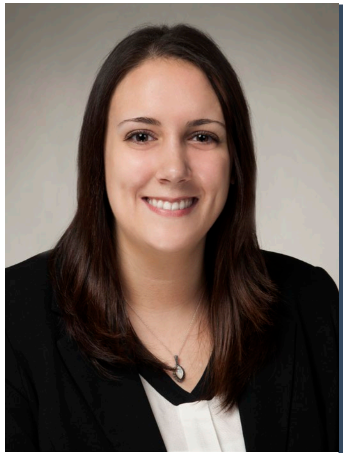
October 26, 2021

Supply Chain Risk Management

Emily Antonico, Krystal Martin, Patrick Morin

BAKER
NEWMAN
NOYES

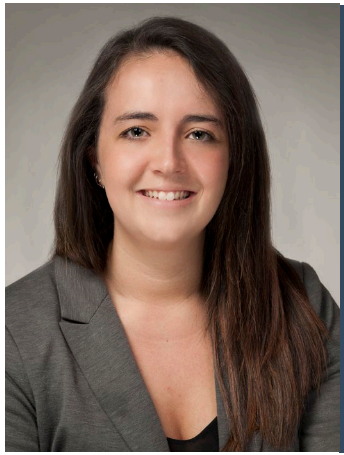
Here with you today



Emily Antonico

Information Systems & Risk Assurance Senior Manager

eantonico@bnncpa.com



Krystal Martin

Information Systems & Risk Assurance Manager

kmartin@bnncpa.com

Patrick Morin

Information Systems & Risk Assurance Principal

pmorin@bnncpa.com

What you'll hear today

BAKER NEWMAN NOYES

1. Types of supply chains
2. What is a supply chain attack?
3. A glance at the headlines
4. Supply chain risk assessment methodology
5. Software Supply Chain Risk
6. A glance “back” at the headlines

Types of Supply Chains

BAKER NEWMAN NOYES

Physical

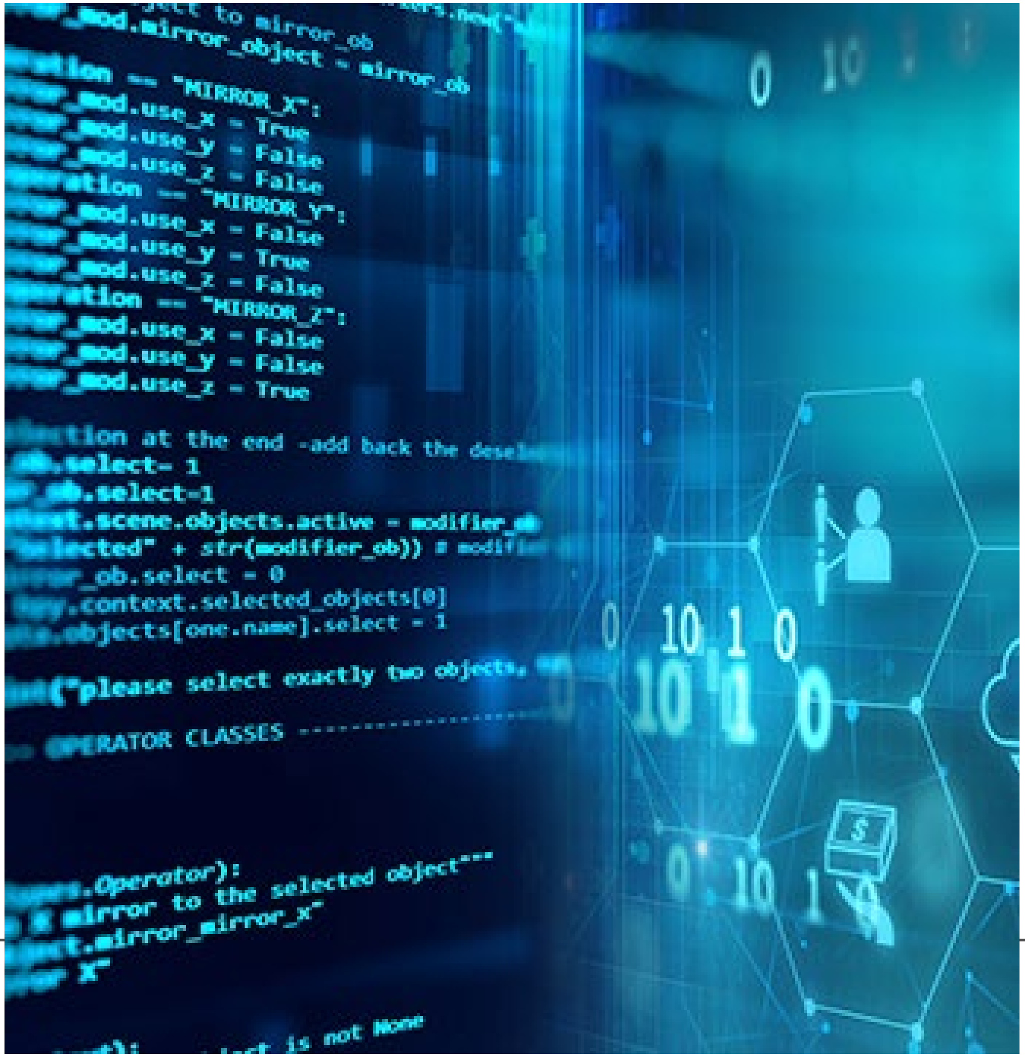
Software

Digital

Physical Supply Chain

- Involves the series of raw materials and processes that are incorporated to create a final, physical product that is delivered to a point of purchase.
- Often those materials and processes are done by a supplier or vendor and then assembled or finished by the final retailer.

Software Supply Chain



- Involves anything that goes into or affects the software that your organization uses and manages.
- From code development, integrations and dependencies and updates until it gets deployed into production (and ultimately into your IT environment).

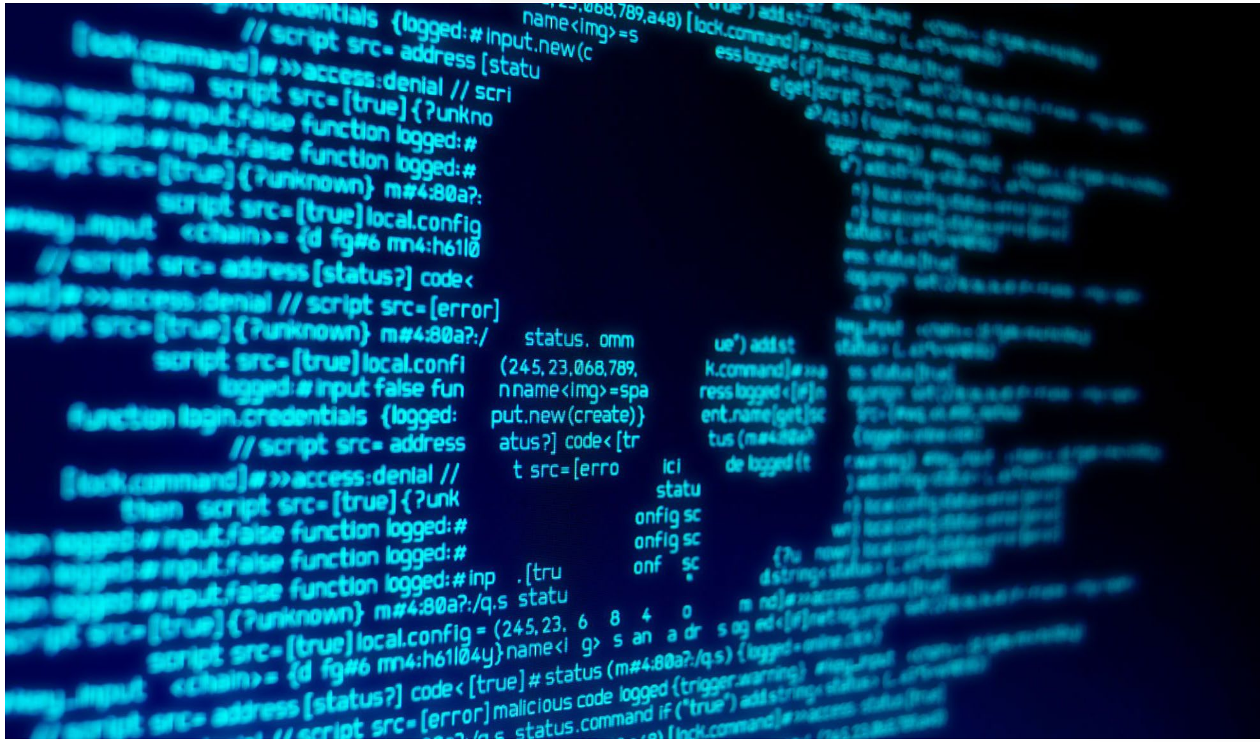
Digital Supply Chain

BAKER NEWMAN NOYES

- Involves the infiltration of your system through a third-party service provider with access to your systems and data that is accessed via the internet or a web-application.

Supply Chain Attack

A ***supply chain attack*** is an attack strategy that targets an organization or its key suppliers through vulnerabilities in its supply chain. It happens when someone infiltrates your system through an outside partner or provider with access to your systems and data.



A Glance at the Headlines

Colonial Pipeline

- In May 2021, a threat actor placed ransomware on the Colonial's billing system.
- The company preemptively shut down 5,500 miles of pipelines causing major disruptions.
- Threat actors were paid $5 million to get the pipeline operational, which proved to be a costly decision; threat actors returned files, but the system remained slow for the coming days.

Solarwinds Orion

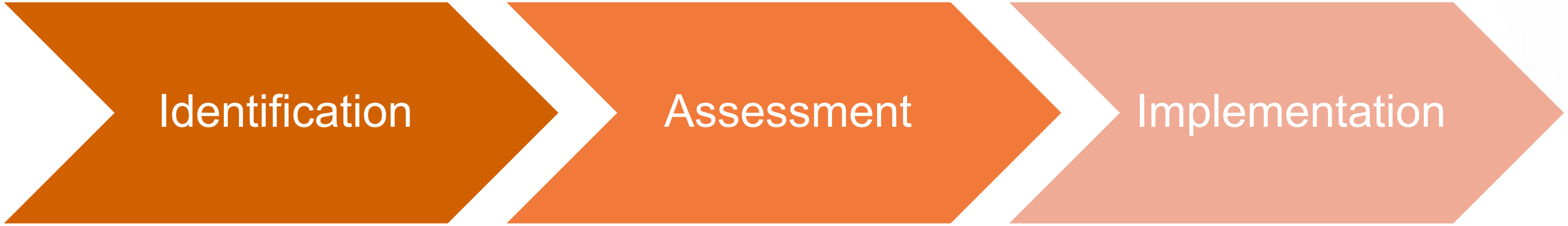
- In 2020, threat actors added malicious code to an upcoming patch that was disseminated to its user base.
- Organizations unwittingly applied this patch to their own systems, allowing the malicious code to infiltrate their infrastructure.
- Victims of this attack included multiple agencies in the US government and fortune 500 companies like Microsoft, Cisco, Intel, and Mimecast.

Mimecast

- In January 2021, a Mimecast-issued certificate used to authenticate some of the company’s products to Microsoft 365 Exchange Web services was compromised.
- The threat actor accessed certain encrypted service account credentials created by customers hosted in the US and UK allowing them to establish connections from Mimecast tenants to on-premise and cloud services.
- This was a direct result of the Solarwinds Orion hack.

mimecast™

Supply Chain Risk Assessment Methodology



Identification

Assessment

Implementation

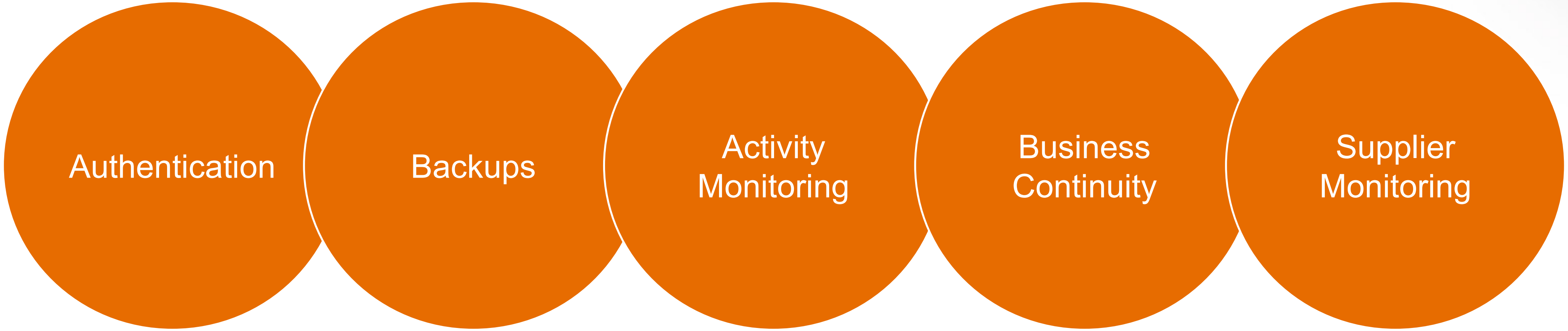
Step 1: Identification

BAKER NEWMAN NOYES

- Identify your suppliers and the risks that exist related to those existing (and potential) vendors and third parties
  - Ensure you have a complete inventory of all providers
- Things to think about
  - What is the nature of the service provided?
  - How critical is the service provided to your organization's ability to supply its own services?
    - What would be the impact of a short disruption vs. a long one
  - Does the vendor or third party have ongoing (persistent) or occasional access to your systems?

Step 2: Assessment

- Assess your organization's ability to mitigate risk in the event of a supplier failure by ensuring that your organization has well developed plans and controls in place relating to the following:



Authentication

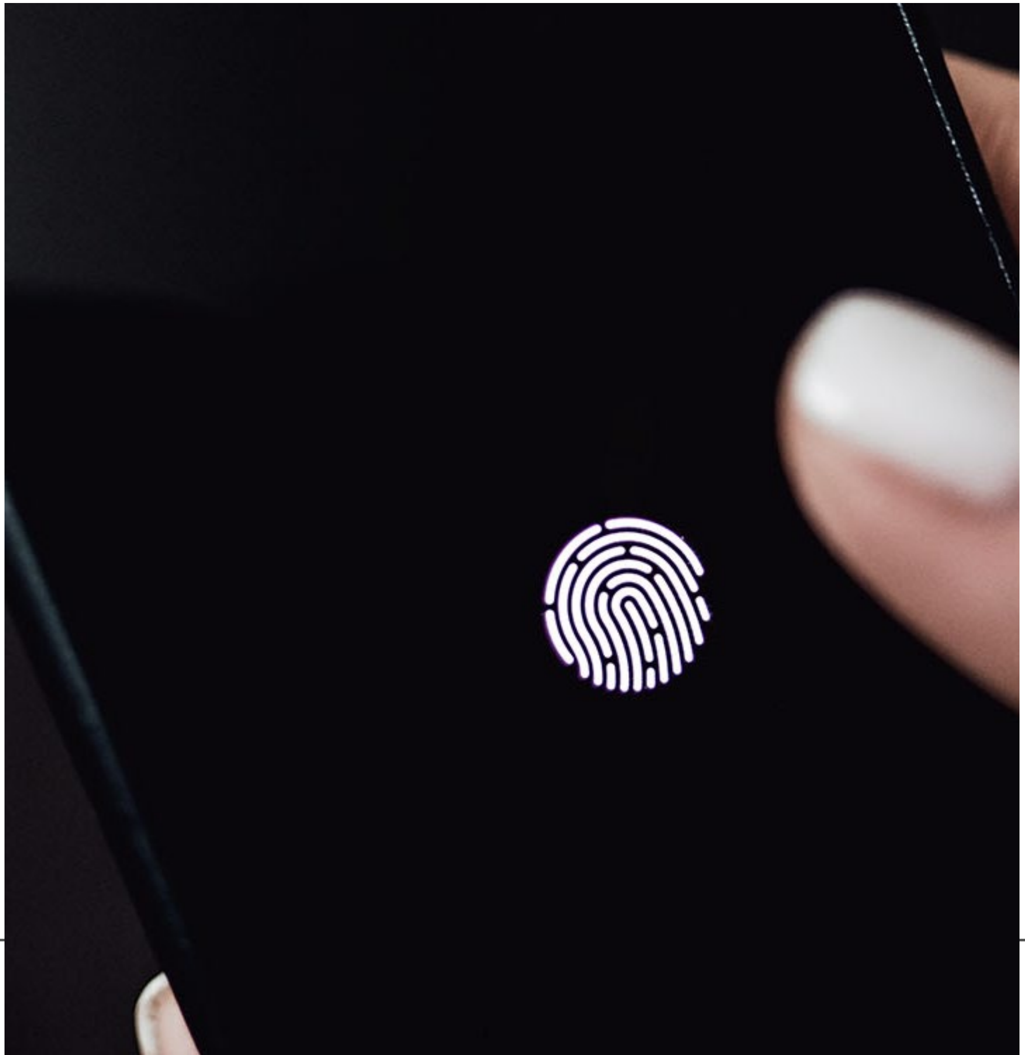
Backups

Activity Monitoring

Business Continuity

Supplier Monitoring

Assessment - Authentication



- Potential controls include using:
  - Unique usernames (no shared accounts)
  - Strong passwords
  - Multi-factor authentication
  - Device identification

Assessment - Backups

- Key considerations include having:
  - Periodic backups of key information
    - Consider using immutable backup solutions
  - Monitoring of the successful completion of the backups in place
  - Retention policies
  - Periodic restore practices

Assessment – Activity Monitoring

- Key considerations include having:
  - Logging enabled
  - An established process to routinely perform reviews of logged activity
    - Account lockouts
    - New accounts
    - Password resets
    - Administrator activity
  - Regular vulnerability assessments
  - Intrusion detection and response plan

Assessment – Business Continuity

BAKER NEWMAN NOYES

- Key considerations include having:
  - A formal plan to follow in the event of an issue or disruption
  - A list of your key suppliers and systems
  - The use of a Disaster Recovery site

Assessment – Supplier Monitoring

- Processes should be in place for both potential new suppliers and for existing suppliers
  - Initial due diligence
  - Ongoing monitoring

Assessment – Initial Supplier Due Diligence

- Evaluate the potential supplier and assign a rating based on impact
  - Critical, high, moderate, low
- Key considerations
  - Operations
    - SOC reports
    - Other third-party evaluation on internal controls
    - Direct inspection or site visit
  - Financial condition
  - Insurance

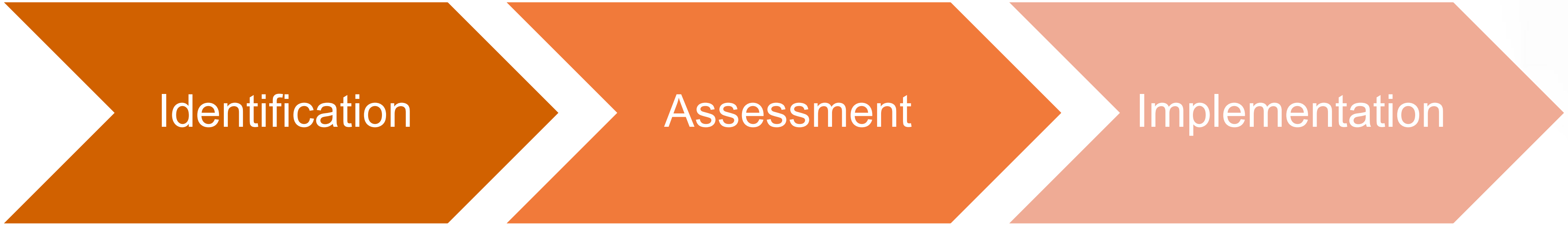
Assessment – Ongoing Supplier Monitoring

The assessment of suppliers is not just reserved for on-boarding. A good supplier risk management program includes processes for the ongoing assessment of suppliers based on their criticality.

Step 3: Implementation

- As your organization performs risk assessments related to supply chain and suppliers, identified risks should be:
  - Documented in a formal risk assessment;
  - Mitigated through the creation and adoption of new controls, policies and procedures; and
  - Reassessed periodically to ensure that the risk is still mitigated and that controls put in place are operating effectively.

Supply Chain Risk Assessment Methodology



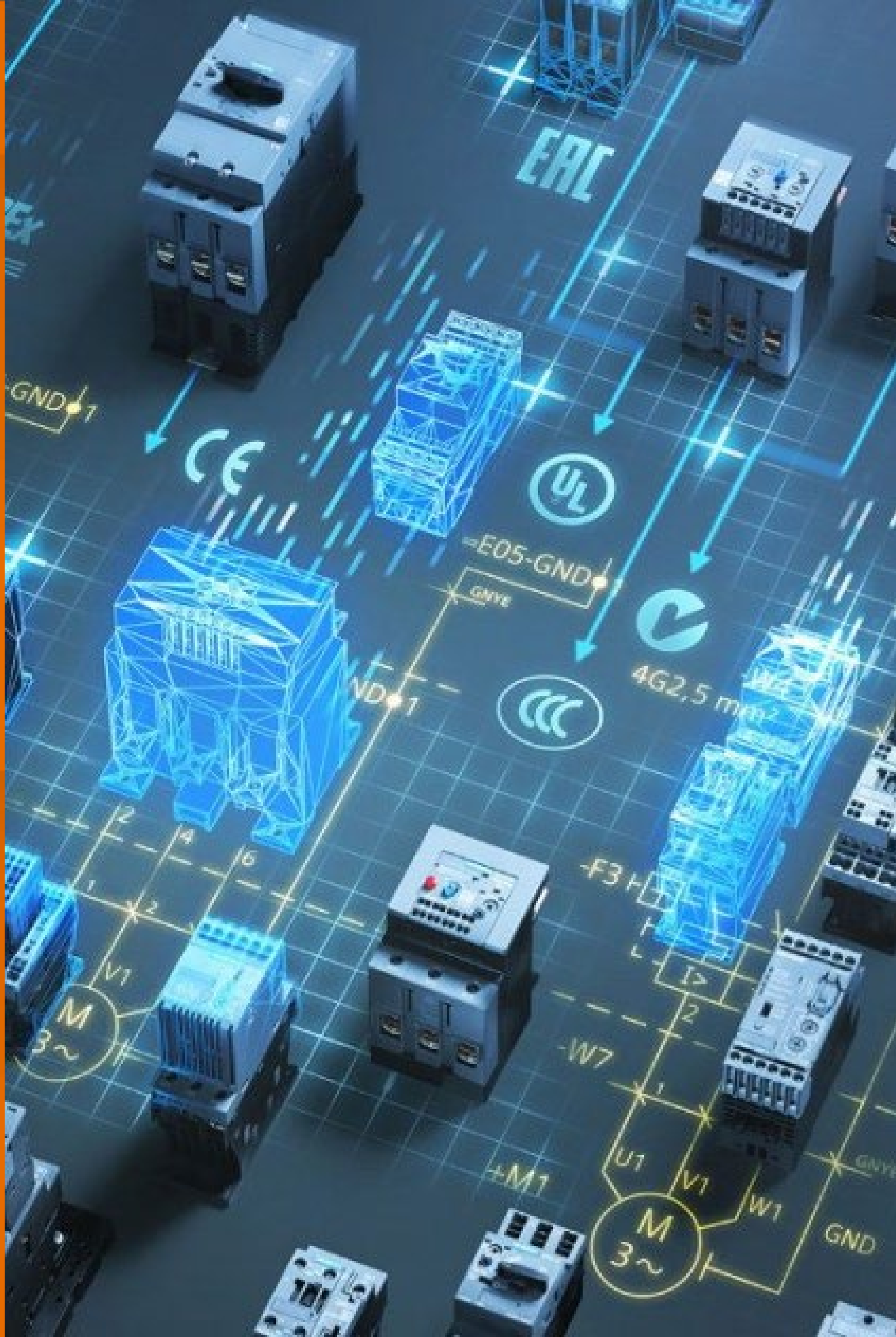
Identification

Assessment

Implementation

BAKER
NEWMAN
NOYES

Software Supply Chain Risk



Software Supply Chain Risk

Common attack techniques in the software supply chain include:

Hijacking updates

Undermining code signing

Compromising open-source code

Software Supply Chain Risk (cont.)

- During the assessment phase an organization should ensure it has:
  - a configuration management program
  - a vulnerability management program
    - including patch management capabilities
  - basic network segmentation to isolate different parts of the enterprise
  - a sound supplier risk management program

Software Supply Chain Risk (cont.)

- Use supplier certifications to determine if the supplier has:
  - a change management program
  - a vulnerability management program
    - patch management capabilities
  - a software component inventory

A Glance “Back” at the Headlines

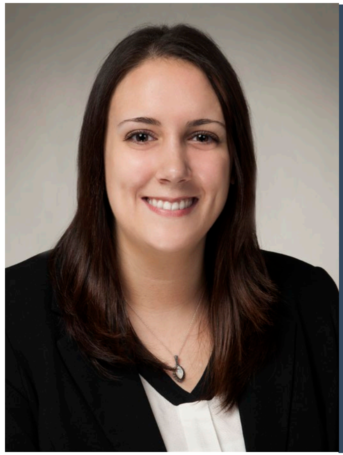
- Strong authentication policies and vulnerability management program may have prevented or identified both the Colonial Pipeline's and Solarwinds' password weaknesses before each fell victim to threat actors that wreaked havoc on the supply chain.
- In the case of Mimecast – a strong incident management program and vulnerability management program was implemented allowing them to catch the threat actor early and stop it from becoming a breach that would have affected much of its user base.

Questions?

BAKER
NEWMAN
NOYES

Disclaimer of Liability: This publication is intended to provide general information to our clients and friends. It does not constitute accounting, tax, or legal advice; nor is it intended to convey a thorough treatment of the subject matter.

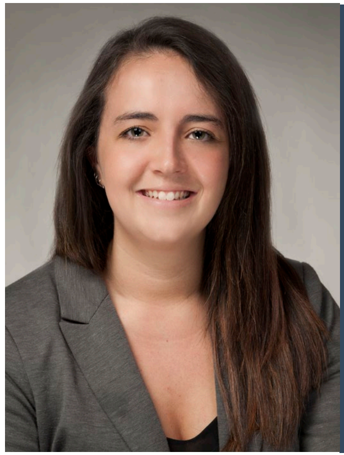
Get in touch!



Emily Antonico

Information Systems & Risk Assurance Senior Manager

eantonico@bnncpa.com



Krystal Martin

Information Systems & Risk Assurance Manager

kmartin@bnncpa.com

Patrick Morin

Information Systems & Risk Assurance Principal

pmorin@bnncpa.com