



Risk & Compliance Solutions | Webinar

Business continuity & incident planning

Emphasizing the ability to adapt to rapid change

Proprietary and confidential. Do not distribute.



Today's panelists



Brianda Rojas-Levering
TruStage™
Risk Consultant
Kentucky



Chris R. Gill
TruStage™
Senior Manager – Risk Management
Maryland



Alex Friedl
M3 Insurance
Cyber Liability Account Executive
Wisconsin

The organizational disruption and costs to identify and resolve incidents — along with the operational downtime and resource impact — can be staggering.

Resiliency



Why build a resilient organization

- Minimize disruption
- Expedite recovery & resumption
- Learn and adapt to more easily navigate future events

How it translates to cyber resilience

- Prepare for the possibility of incidents or breaches
- Ensure systems can withstand disruptions
- Validate contingency plans
- Recover quickly
- Minimize impact

Why it matters...

Despite the best defenses, incidents can and do occur.



A well-executed incident response plan helps minimize damage and ensures faster recovery, protecting both operational integrity and customer trust.

Cyber resilience framework





- Regularly conduct risk assessments,
- Develop and conduct Business Impact Analysis
- Develop incident response and disaster recovery plans
- Maintain strong cybersecurity hygiene
- Ensure employees are trained to recognize and respond to threats
- Test and validate

Importance of focusing on preparation



If you fail to plan,
you are planning to fail.

**Incident response
planning is your
roadmap to help
your intake,
evaluate and
respond.**





Incident plan elements

- Apply your organization's specific business objectives and priorities
- Identify the potential events that could affect your business
- Grade risks according to the impact
- Highlight a strategy that can be implemented to mitigate and manage risks
- Pinpoint key performance, success, or service-level indicators or metrics
- Explain who's on the response team – and how and what will be communicated
- Understand how partner/vendors, including insurance, will respond and adapt



What are some common mistakes when planning?

Meg in Indiana

Common mistakes or oversights



- Incident response plan is closely held and not communicated to all staff
- Not gaining leadership buy-in to the importance of developing, testing, and maintaining an incident response plan
- Lack of testing or going deep enough with scenarios in testing
- Not considering potential response delays (e.g., access issues; escalation bottlenecks)
- Remember, operations change, risks change, and so might your incident response plan



From a cyber insurance perspective,
are there any key considerations?

Other important considerations

- Understand what you'll do if you're notified that PII stored with a third- or Nth-party has been accessed by a threat actor
- Maintain a list of key contacts and multiple communication methods within your plan – including preferred vendors/partners
- Keep a printed copy of your plans (maybe multiple) and know where to find them
- Notify your insurance carrier as soon as possible
- Always obtain approval prior to incurring expenses related to an incident





Other than training, how do you get more engagement from departmental managers?

Elaine in Florida



Business Impact Analysis (BIA)

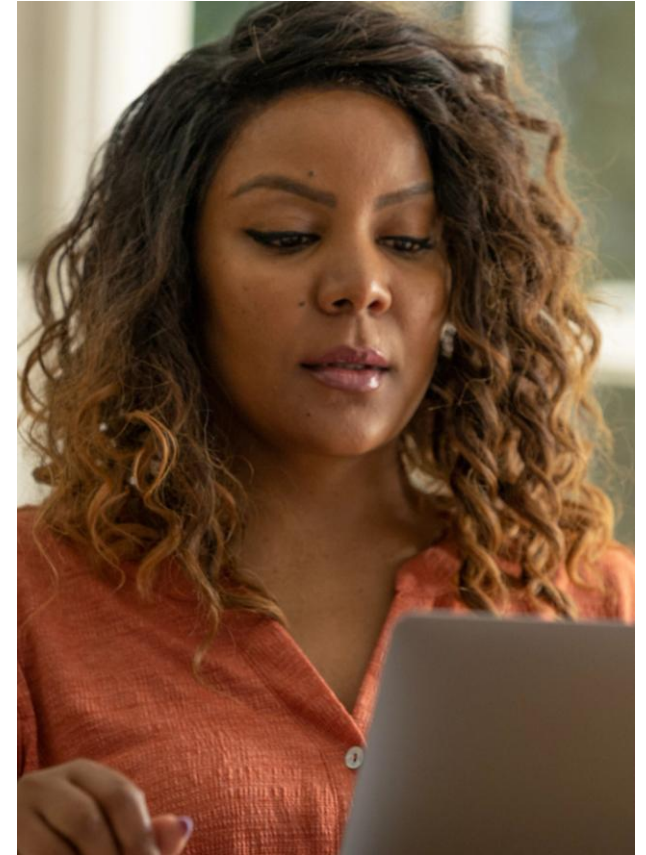
Business impact analysis (BIA)



- Creates a picture of potential impacts and organizational effects in the event of an interruption to critical business functions
- Quantifies how long it should take to recover
- Helps with fact-based decisions



- NCUA suggests including:
- Critical system or service
 - Types of failure events
 - Minimum acceptable services levels or system output
 - Probability of occurrence
 - Probable timing of the occurrence
 - Cost, duration & impact



Typical BIA



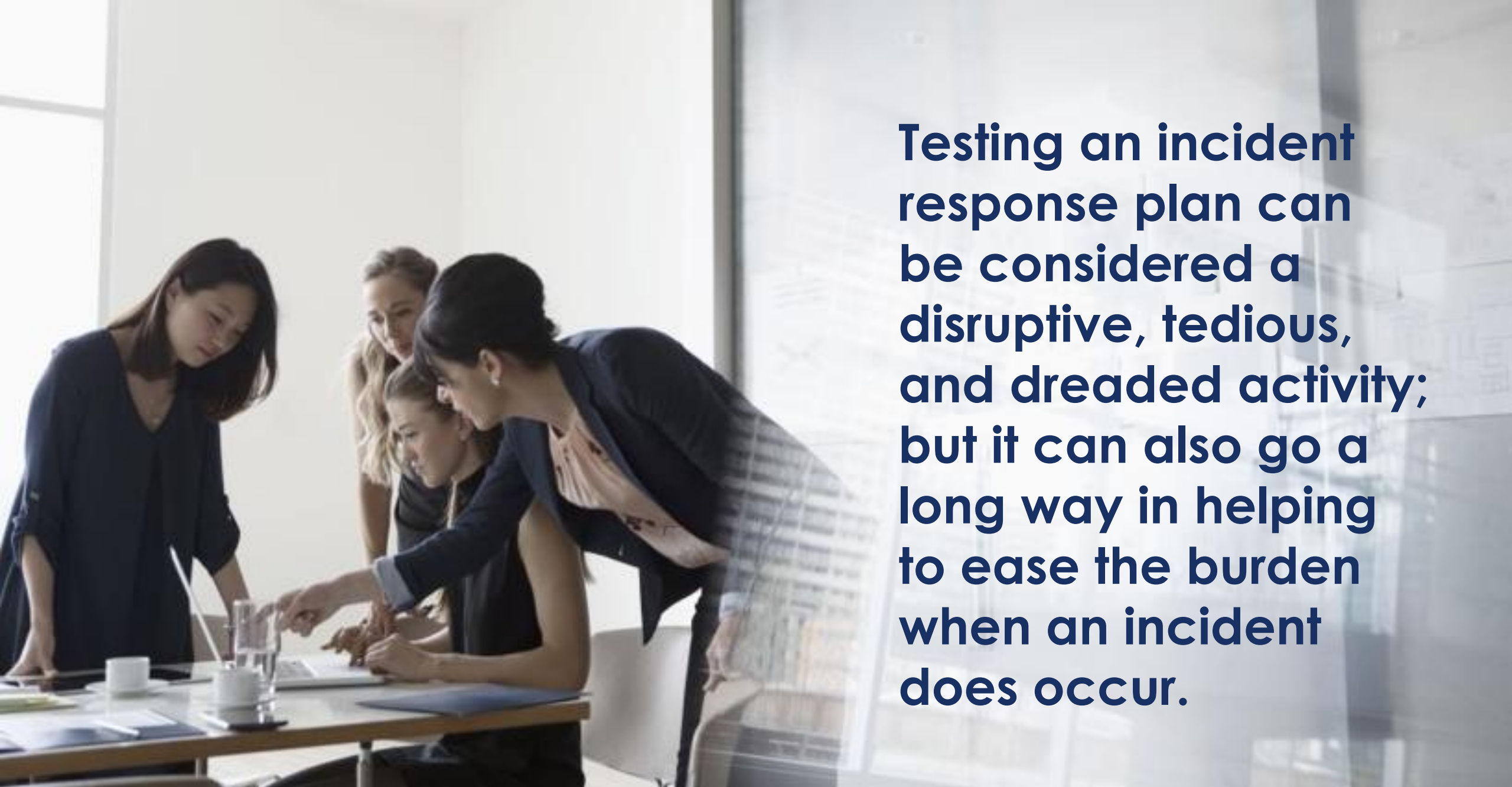
- Department(s)
- Services or function impacted
- Criticality or importance to the organization's business operations
- Maximum Allowable Downtime (MAD) or Max Tolerable Downtime (MTD)
- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)
- Costs/financial loss

A tip to consider:

Maintain a list of critical third-, 4th and Nth-parties to help provide you with risk concentration for critical service providers and better understand the impact of a vendor incidents.

Some resources to help:

- [Business resilience planning guide & checklist](#)
- [Business continuity tabletop training exercises](#)
- [Disaster response & communications risk overview](#)
- [Incident response tabletop exercise & discussion guide](#)
- [Third-party vendor cyber incidents risk overview](#)
- [Root cause analysis investigation checklist](#)



Testing an incident response plan can be considered a disruptive, tedious, and dreaded activity; but it can also go a long way in helping to ease the burden when an incident does occur.

Importance of testing



- Validate strong controls and processes
- Identify weaknesses
- Minimize surprises
- Allow team to practice
- Enhance understanding of new concepts
- Promotes in-depth discussions
- Keep leadership informed



What do you recommend for performing tabletop or other testing exercises?

Karla in New Mexico



Testing options

Document Review

Review recovery plans, procedures & other related business continuity/resiliency policies seeking out weaknesses or missing components

Tabletop Exercise

Conduct a live, mock scenario where team members are required to demonstrate their duties, in addition to identifying gaps and/or weaknesses

Walk-through drill

Run a hands-on version of the tabletop exercise incorporating actual recovery actions such as restoring backups, live testing of redundant systems, and any other relevant processes

Functional recovery test

Go through the complete process of spinning up your backup systems and processing transactions or data.

Realistic scenarios are the centerpiece of the testing exercise – often making it a memorable and valuable experience for everyone involved. Throwing in a series of **developments or twists** can heighten the realism and assist understanding of potential consequences.



- Ransomware
- Cyber extortion
- Insider threat
- Information stealing trojans
- Software vulnerability exploitation
- Cloud-based data breach
- Vendor supply chain compromise

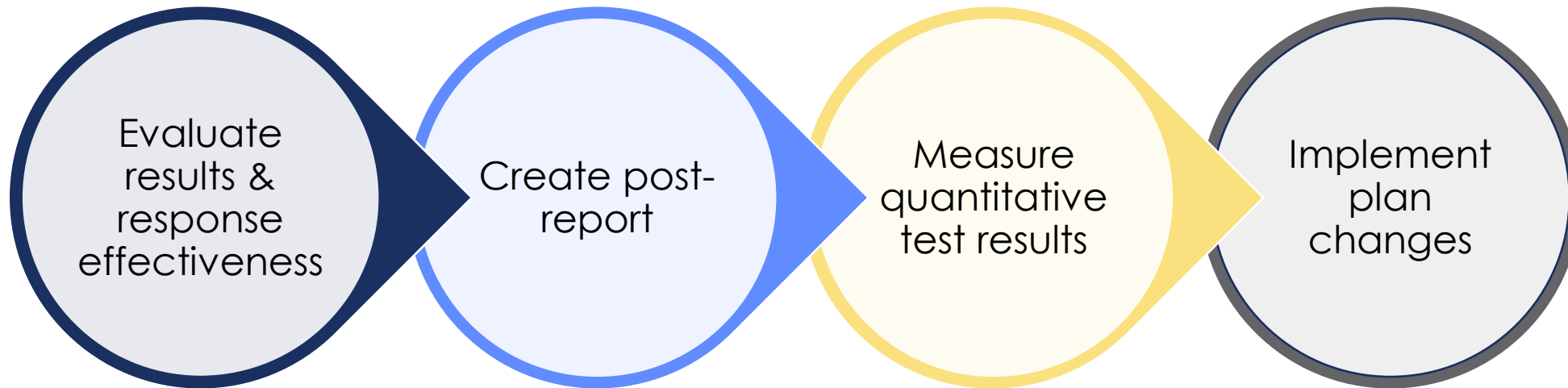
Popular cyber incident scenarios

Keys to effective testing

- Develop an actionable playbook to guide the testing process
- Set clear expectations and define success criteria
- Prepare a draft test plan with detailed information about the test
- Secure management approval, support, and funding for the test
- Schedule time for the environment that will be tested and verify that it's ready when it's testing time
- Document what happens during the test including what worked & what didn't work
- Debrief and ask for employee feedback following the test
- Build variety into testing plans



Critical next steps after testing

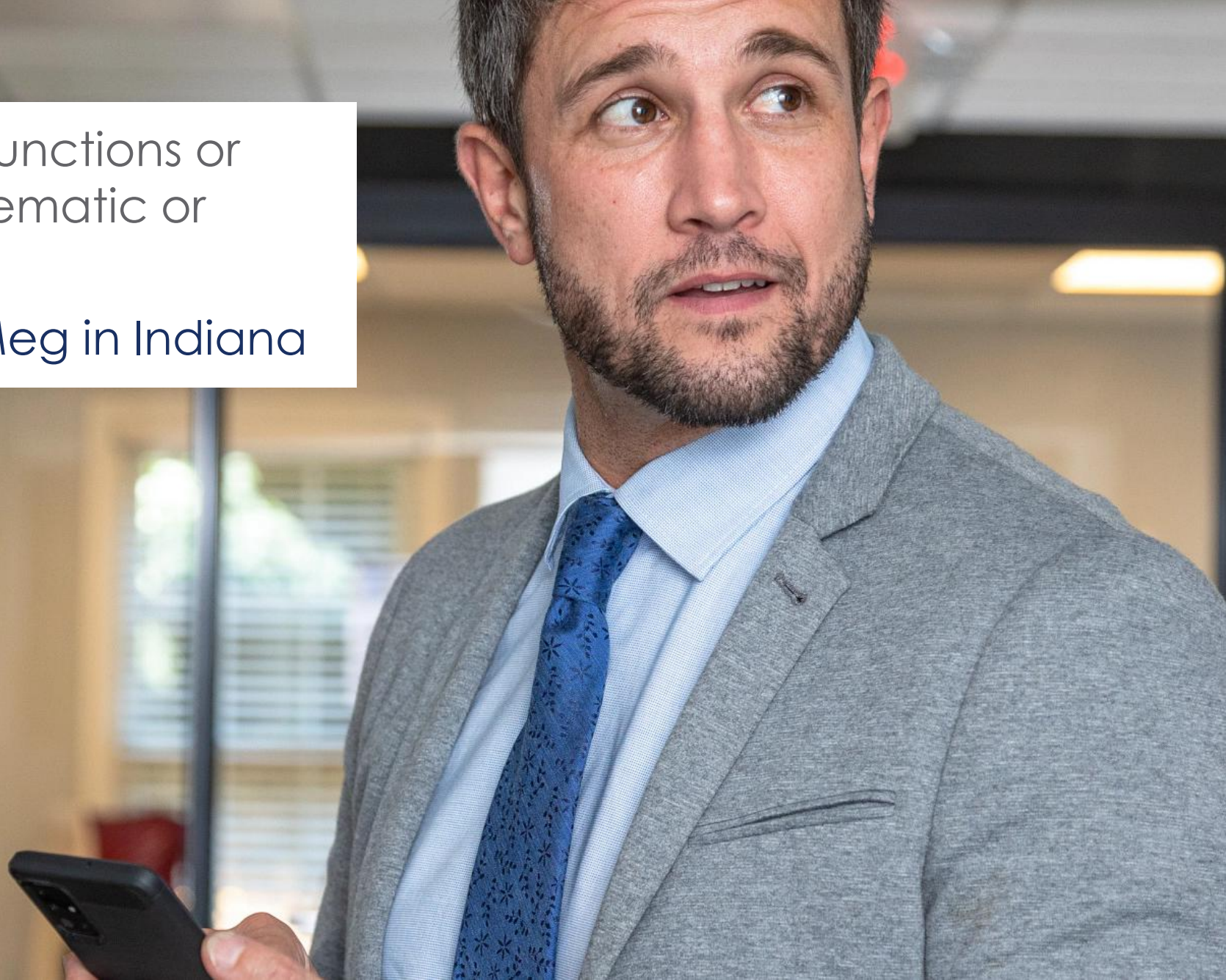


How often should updates regarding plans be provided to executive management?

Elaine in Florida

Have you found specific functions or areas that are most problematic or most overlooked?

Meg in Indiana





Detection is critical even during planning stages

Monitoring systems sensitive to unusual activities or known threats quickly raise an alert to the response team for immediate action and containment of the threat

- Intrusion Detection Systems (IDS)
- Security Information and Event Management (SIEM)
- Endpoint Detection and Response (EDR)
- Network Traffic Analysis (NTA)
- Threat Intelligence

→ **Continuous monitoring is needed**

Recovery should be in the plans



- **Repair vulnerability** - After containing the incident or breach, it's crucial to address the vulnerabilities that were exploited
- **Restore affected systems** - Focus on restoring affected systems by recovering data from backups. Ensure that backups are recent and uncorrupted
- **Maintain planned service levels** when possible
- **Communicate with affected parties** - Provide updates and next steps to employees and members as soon as possible. Transparency is key. Inform them about what happened, how it affects them, and what steps they should take to protect themselves.



Should we communicate incidents to the media?

Communication considerations



- Develop a clear, simple and credible narrative describing the actions you will take to confront an incident or reputation risk
- Identify an authorized spokesperson to make statements, comments or declarations externally or internally to members, vendors, or media outlets
- Ensure all staff can communicate the message efficiently and effectively
- Before releasing any statements, have language reviewed by an attorney or public relations firm
- Maintain holding statements in your incident response plan
- Do not use the word “breach” as this can designate a legal meaning

A photograph of three people in an office setting. In the foreground, a woman with long brown hair and glasses is looking at a computer screen, her hand resting on her chin in a thoughtful pose. Next to her, another woman with long dark hair and glasses is also looking at the screen, appearing to be in the middle of a conversation. To the right, a man with a beard and dark hair is partially visible, looking towards the same direction. The background is slightly blurred, showing other office equipment and a person in the distance.

When should we notify membership?
Are there any policy best practices?

Patty in Indiana

Risk resources

Business Protection Resource Center www.trustage.com/bprc

- RISK Alerts – warning | watch | awareness
- Loss prevention library
- risk overviews, checklists & whitepapers
- Emerging risks outlook
- Live webinars, risk forums & office hours
- On-demand learning & interactive training modules

“Great information, excellent format. Presenters were engaging and knowledgeable in their respective fields.”

Executive Vice President - \$3B credit union



Root cause analysis

Investigation checklist

Document as early, as much, and as often as you can. The purpose of the initial investigation is to determine the threat level and classification of the incident.

The threat levels are not intended to be overly rigid. It's impossible to capture every type of potential incident and taking too long to determine where a specific incident falls only wastes much needed time. Incident response is fluid.

Type

- ☐ System access
- ☐ Data loss
- ☐ Disruption of service
- ☐ Structural or property damage or destruction
- ☐ People impact

Criticality

- ☐ Confirmed incident/critical systems
- ☐ Confirmed incident/critical operations
- ☐ Confirmed incident/non-critical systems
- ☐ Confirmed incident/increased expenses
- ☐ Possible incident/non-critical systems
- ☐ Possible incident/non-critical operations

Sensitivity

- ☐ Extremely sensitive/confidential
- ☐ Sensitive/internal use

Potential log inputs

- Date
- Description
- Type
- Sensitivity
- System/function/user impact
- Anticipated resolution
- Input name
- Owner
- Criticality
- Duration
- Financial impact
- Date completed



Incident response

tabletop exercise & discussion guide

Cyber threats, such as ransomware, distributed denial-of-service (DDoS) attacks, and supply chain interruptions, have provided organizations an opportunity to reclaim and reinvigorate incident response planning. While there is no one correct way to develop and test your incident response plans, it is important to continuously improve the plan by incorporating lessons learned.

Tabletop exercises for incident plans use a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. These resources assist you to initiate discussions within your organization about your ability to address a variety of cyber threat scenarios.

Cyberattacks can cripple networks and jeopardize critical aspects of your organization. Incident response plans must emphasize speed and flexibility, so you are able to quickly adapt to rapid change.

Each exercise and scenario are customizable and should involve discussion questions to assist your key stakeholders with the ability to identify gaps and potential issues.

It is essential that your leadership and employees use fact-based information and tested alternatives to enable real-time decision making. This integrated, comprehensive approach will help you build long-term operational resilience and prepare the credit union organization for any future cyber disruption.

Clearly, there is a lot at risk when it comes to incident response planning.

Do you know what to do if you are a victim?

An incident response plan is a critical component in your ability to take the necessary actions to respond to data breaches efficiently.

Establish a core vision that is tailored to your credit union's specific business objectives and priorities. However, your focus must go beyond vision and theory, you need application.

Testing your incident response plan's level of resilience can be strengthened by identifying the potential events that could affect your business, grading risks according to the impact, and then implementing a strategy to mitigate and manage risks.

And your partners are crucial to the resilience of the credit union. Understanding how partner/vendors will respond and adapt to change will contribute to improved resilience.

Remember, a tabletop exercise isn't an exam. It should be a convincing simulation that lets your team practice working through your incident response plan and identifying needed changes in that plan.

The incident response tabletop exercise is built around the concept that your organization likely will be impacted by some sort of cyber incident and proactive preparation will help minimize the damage.



Cybersecurity Alert

Actionable insights in an era of uncertainty

Awareness

Watch

Warning

Pixel tracking class action litigation catches some organizations by surprise

Class actions targeting organizations - including credit unions - for their use of digital tracking and web analytics technologies such as session replay tools, chats, and now tracking pixels continue to increase. Recent class action lawsuits and litigation allege that the use of pixel tracking technologies violates certain state and federal privacy laws.

Alert details

Tracking pixels, also known as web beacons, are usually transparent, hidden, or embedded pixel graphics or images present in the background of a website, email, or cookie banner ads. Tracking pixels can track and send a variety of data, for example, how a user interacts with a web page including specific items purchased. Commonly used for marketing or web analytics, the use of pixels helps track consumer behavior on websites such as pageviews, clicks, and interactions. They can assist businesses to better target offerings or monitoring messages to users based on their previous online behavior. Two widely used pixels are the Meta (Facebook) and Google pixels.

Regulatory action and class action lawsuits against to pixels and other website technologies has surged particularly within the healthcare industry; however, some credit unions have reported increasing demand when suggesting class action litigation. Some plaintiff attorneys are using various state privacy statutes and federal laws such as the Electronic Communications Privacy Act of 1986 (ECPA), Criminal Fraud and Abuse Act of 1986 (CFAA), Video Protection Privacy Act of 1988 (VPPA) and others, for claims that these tracking technologies record or intercept user interactions without consent, thus, violating state and federal laws.

The allegations in pixel litigation cases vary, but primarily allege that organizations collect, use, and disclose personal information of consumers who browse their website without their consent.

- visitors
- organs
- the rec
- the coo

Adding to it
Plaintiff are
information
addresses, i

Date:
March 25, 2023

Risk category:
Data privacy lawsuits; Class action; Litigation; Cybersecurity; Pixel tracking

Status:

All

Share with:

- Executive management
- IT
- Legal/compliance
- Marketing
- Risk manager
- Web development



Risk & Compliance Solutions | Presentation

Emerging risks outlook

Rethinking protection in an era of uncertainty

Proprietary and confidential. Do not distribute.





Contact us

800.637.2676

- riskconsultant@trustage.com
- [Ask a risk manager interactive form](#)
- [Schedule a 1:1 risk consultation](#)
- [Report a risk or scam](#)



Thank you.

Contact

riskconsultant@trustage.com

800.637.2676

This presentation was created by the CUNA Mutual Group based on our experience in the credit union and insurance market. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value and implementing loss prevention techniques. No coverage is provided by this presentation/publication, nor does it replace any provisions of any insurance policy or bond.

TruStage™ is the marketing name for TruStage Financial Group, Inc., its subsidiaries and affiliates. TruStage Insurance Products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company. Cyber policies are underwritten by Beazley Insurance Group or other nonaffiliated admitted carriers.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy. Please read the actual policy for specific coverage, terms, conditions, and exclusions.