TruStage®

Risk & Compliance Solutions | Webinar

Business continuity & incident planning

Emphasizing the ability to adapt to rapid change

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

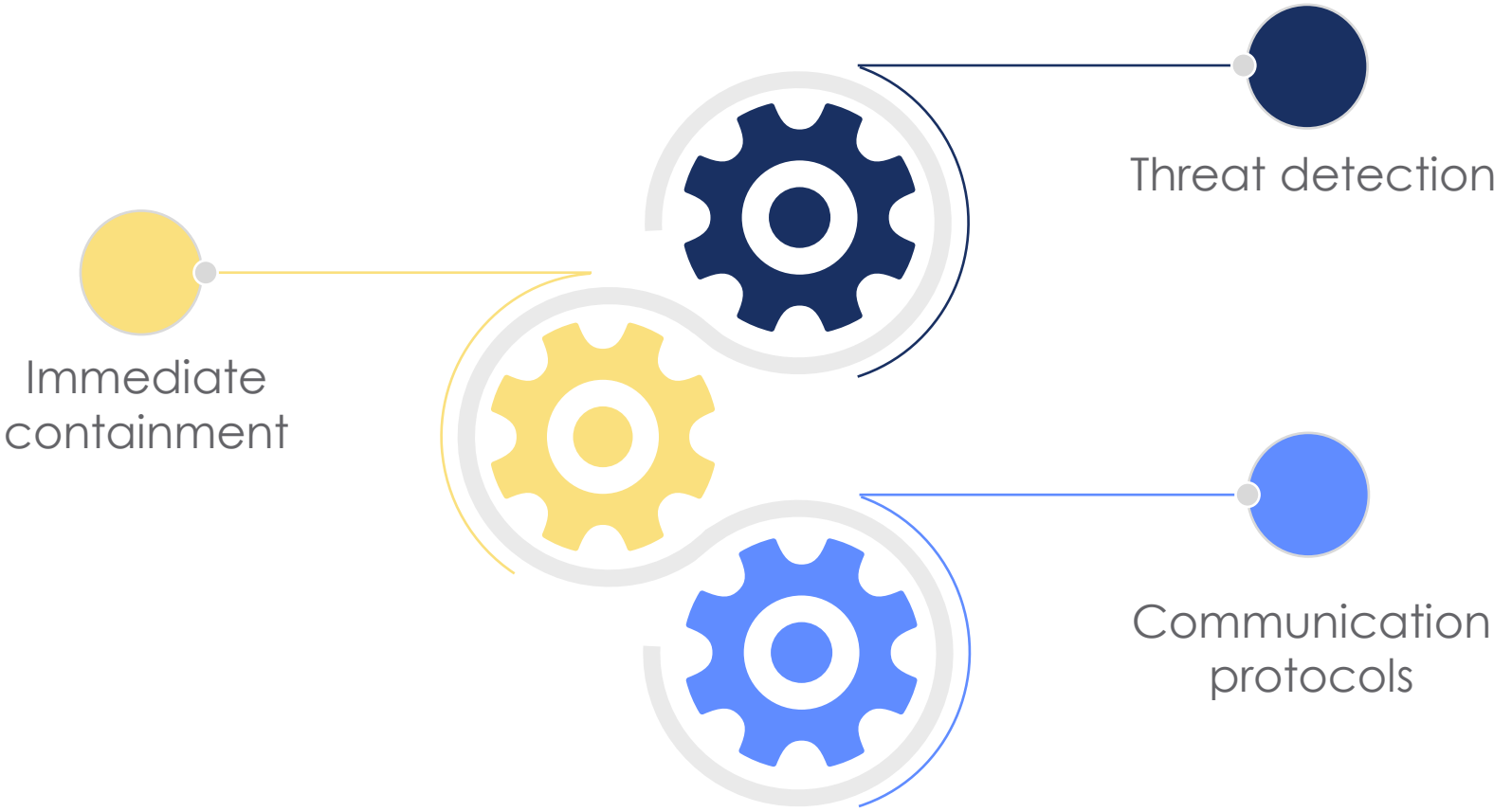
- Minimize disruption
- Expedite recovery & resumption
- Learn and adapt to more easily navigate future events

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 wow 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

TruStage®

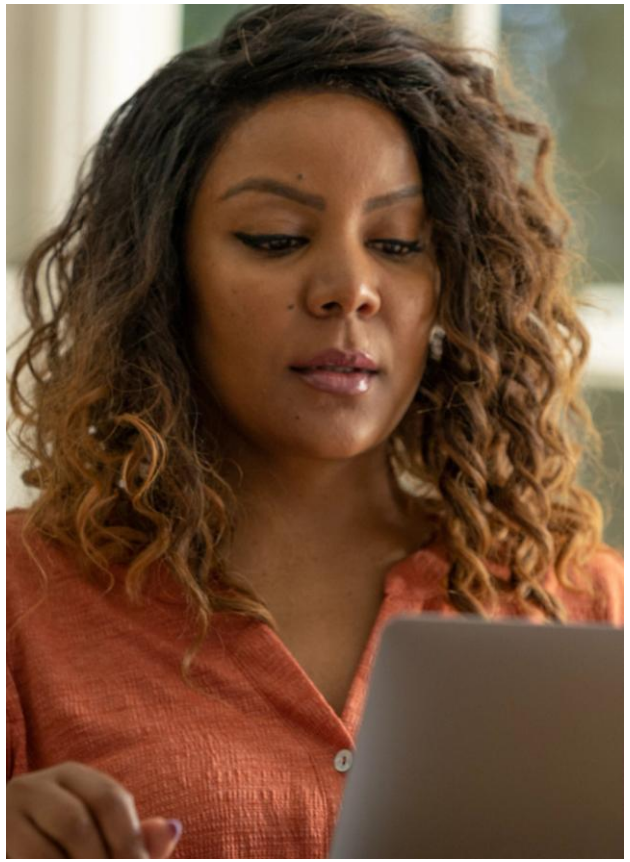
Business Impact Analysis (BIA)

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

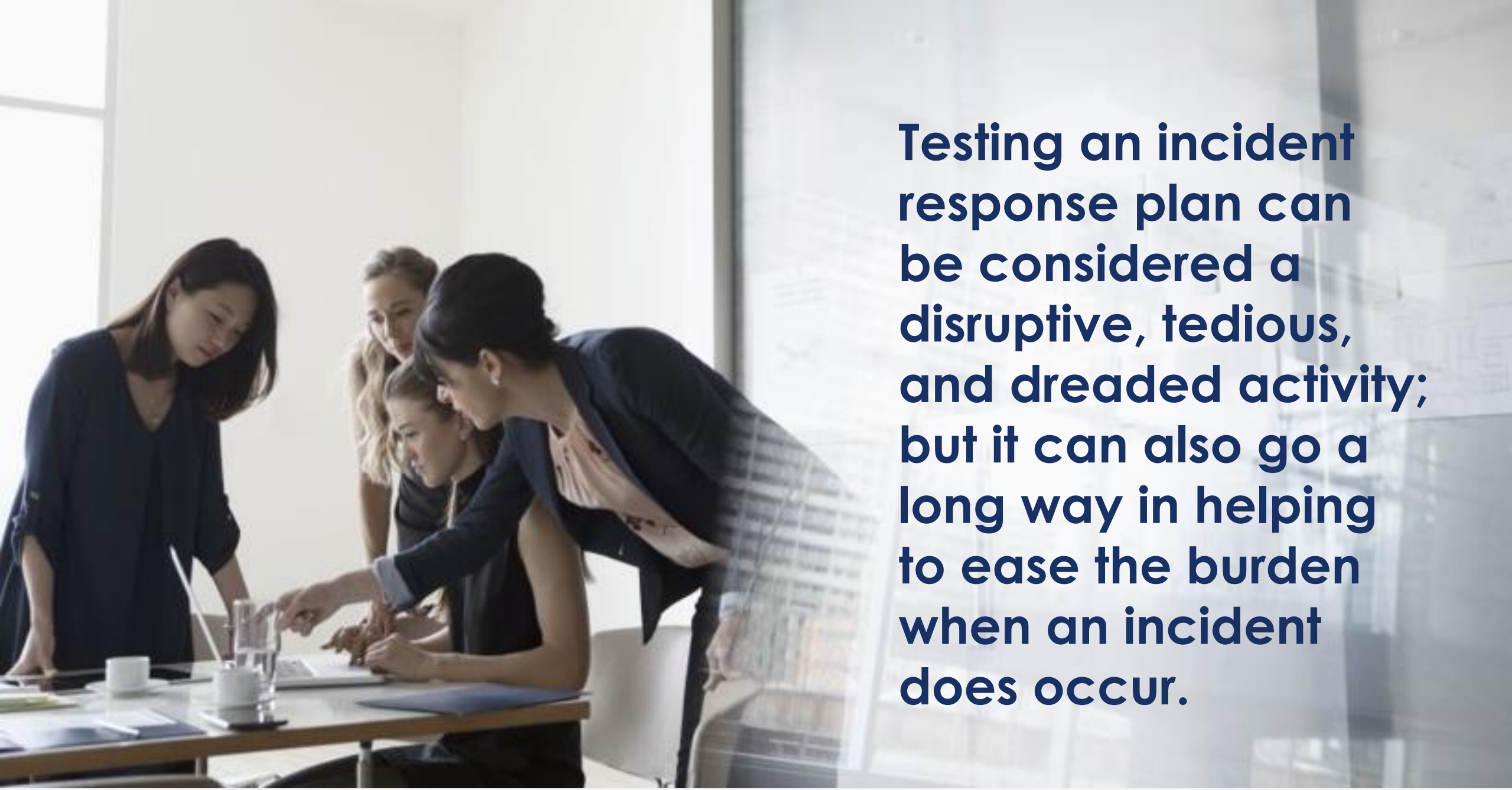
- Department(s)
- Services or function impacted
- Criticality or importance to the organization's business operations
- Maximum Allowable Downtime (MAD) or Max Tolerable Downtime (MTD)
- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)
- Costs/financial loss

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	Tabletop Exercise	Walk-through drill	Functional recovery test
Review recovery plans, procedures & other related business continuity/resiliency policies seeking out weaknesses or missing components	Conduct a live, mock scenario where team members are required to demonstrate their duties, in addition to identifying gaps and/or weaknesses	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	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.

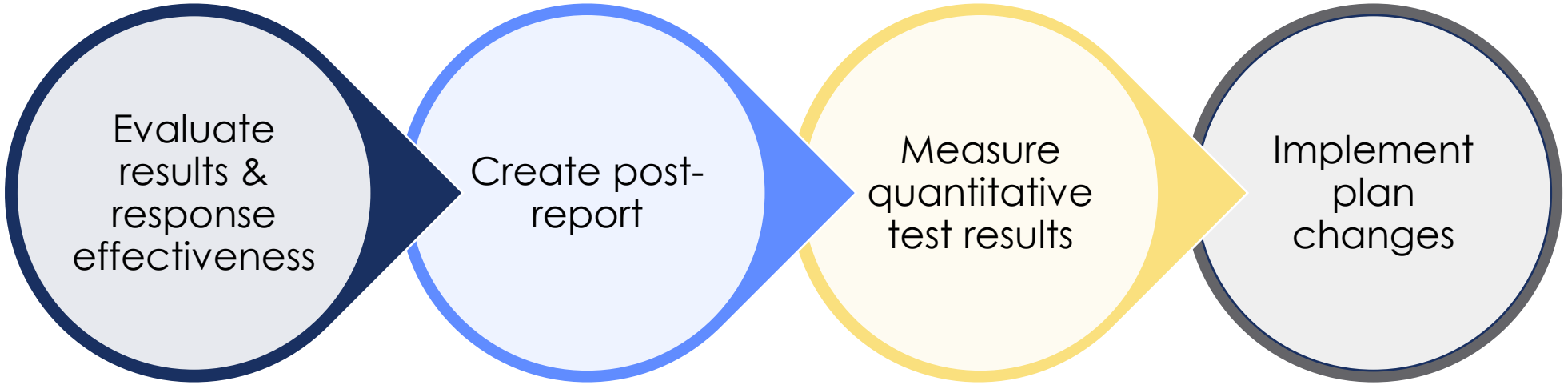
- Ransomware
- Cyber extortion
- Insider threat
- Information stealing trojans
- Software vulnerability exploitation
- Cloud-based data breach
- Vendor supply chain compromise

Popular cyber incident scenarios

Keys to effective testing

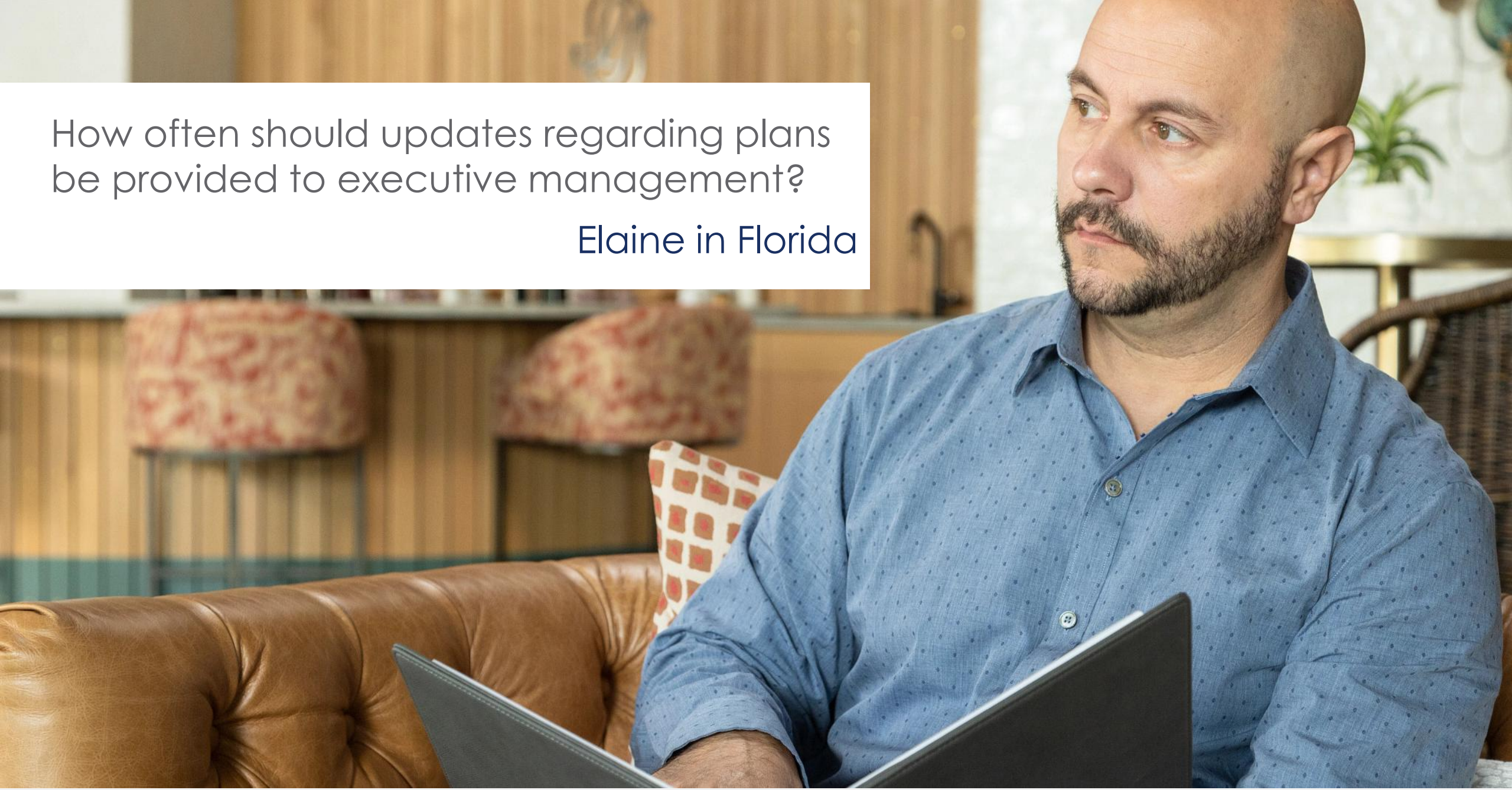
- Develop an actionable playbook to guide the testing process
- Set clear expectations and define success criteria
- Prepare a draft test plan with detailed information about the test
- Secure management approval, support, and funding for the test
- Schedule time for the environment that will be tested 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

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

Patty in Indiana

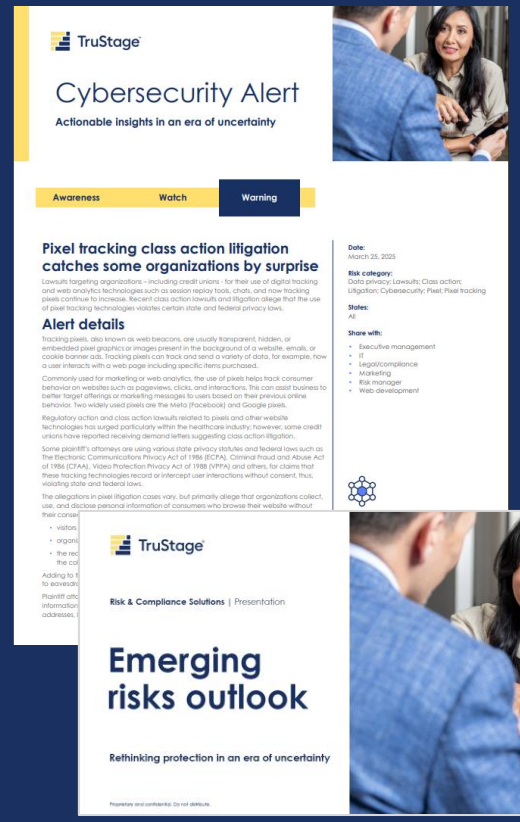
Risk resources

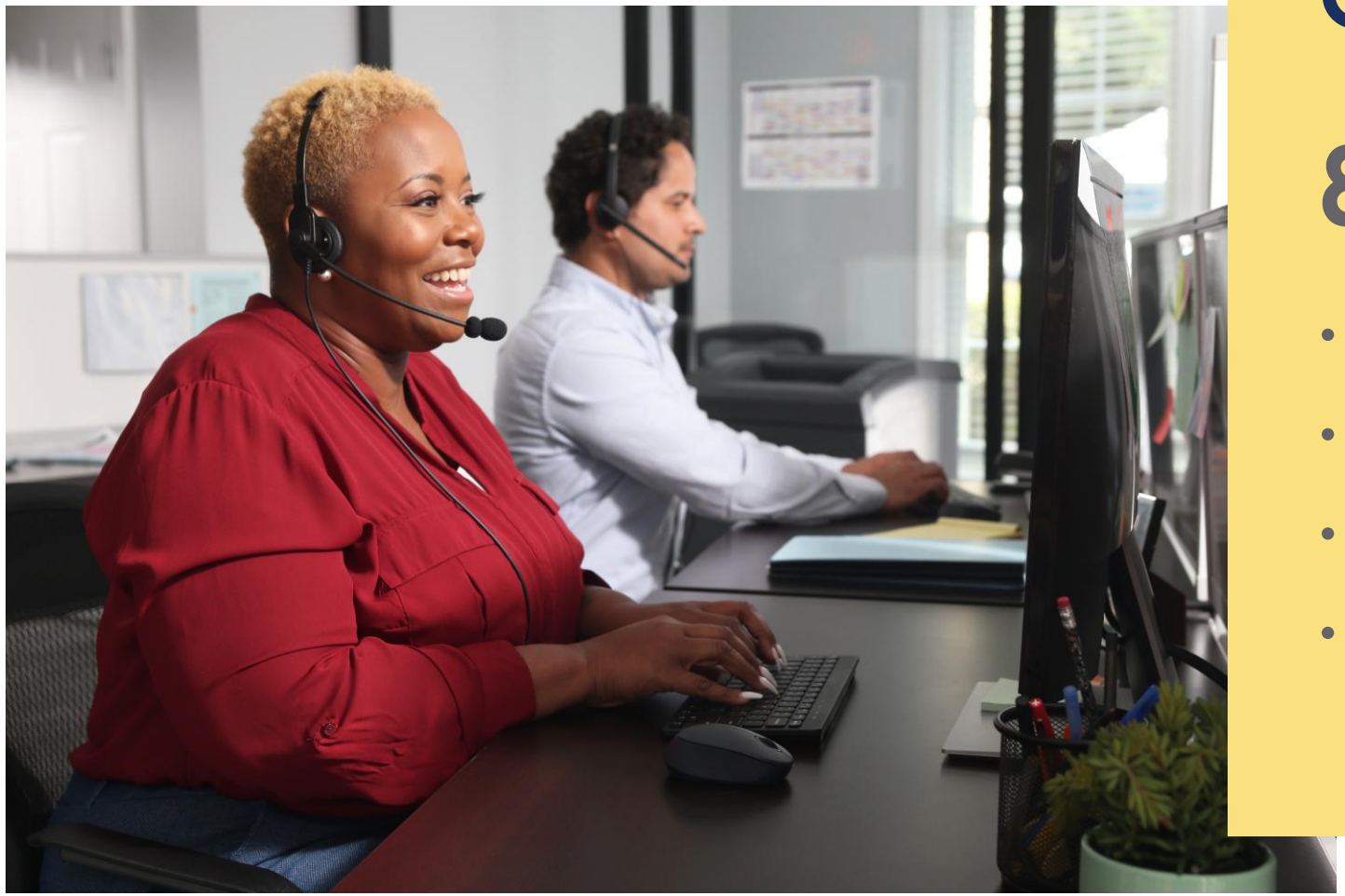
Business Protection Resource Center
www.trustage.com/bprc

- 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





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

TruStage®

Thank you.

Contact
riskconsultant@trustage.com
800.637.2676