peters & associates
simplify solve succeed

Incident Response Plan (IRP) **Modernization Checklist**

7 ways to self-assess whether your IRP is up to date.

It's Not a Matter of If, But When...

The sensitive nature of financial information means that financial institutions are an irresistible target for bad actors. Having an incident response plan is both essential to minimizing disruptions and required by federal regulators.

Every Incident Response Plan should have these 7 elements. Use this checklist as a guide when assessing your IRP's viability.

- ☐ **1. Incident Identification**
  Have you defined the differences between an event and an incident? ALL incidents are events, but NOT all events are incidents. Where do events get reported and which group will use the criteria to determine if the event is an incident?

- ☐ **2. Assessment of the Nature and Scope of the Incident**
  After an event has been determined to be an incident, a cursory but rapid evaluation of the incident must be done. Who will conduct this? What questions should be answered? What is the current and potential impact of the incident? What assistance is needed to determine next steps?

- ☐ **3. Lessons Learned**
  Like a story, every incident has a beginning, middle, and an end. All incidents should have a post-mortem where the group can discuss and document to file key Learnings. Unfortunately, this is one of the most omitted IRP activities, and it is one of the most important as it fuels improvement and development. Not only is it the perfect time to address any gaps that you found within your existing IRP, it also provides valuable training material.

- ☐ **4. Annual Review and Testing**
  Thinking responses through and committing to paper is 50% of the solution. The other 50% is testing and updating procedures annually, or more often if circumstances dictate. Tabletop testing how your team reacts is step one. Testing can be deepened with additional variables, such as Layered incidents (data theft AND ransomware) or personnel unavailable (pandemic flu).

5. Responses to Specific Scenarios

Modernize your approach with current incident responses. All organizations have high likelihood of experiencing a cyber event (ransomware or business email compromise) or a human operations event (pandemic flu). You can further explore industry-specific incidents such as 3rd party data mishandling, unencrypted emails with personal information, etc.

6. User Awareness and Training

Employees-Users should be made aware of policies and procedures regarding acceptable use of computer networks, systems, and applications. Applicable lessons learned from prior incidents should also be shared with employees so they can see how their actions could impact the entire organization. As always, users are the most important link in the cyber-security chain.

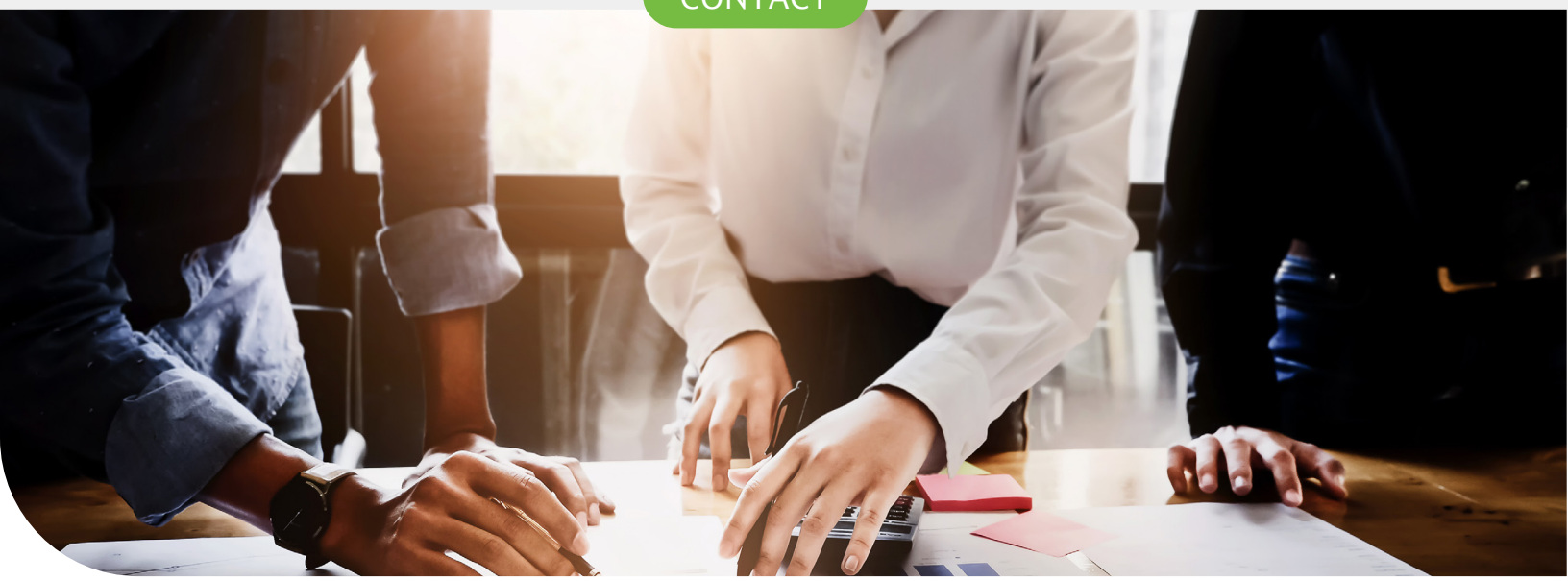
7. Cyber-Insurance Review

The organization should easily be able to identify who is responsible for the policy, coverage levels, what is in/out of coverage, as well as which breaches require forensics and does it pay for recovery services. An annual review of policy parameters with the Incident Response team and incorporating insurance into annual testing is a logical approach.

Develop a Plan With Peters & Associates

Developing a thorough incident response plan takes time and expertise. At Peters & Associates, we have almost four decades of experience working with organizations to improve their security stance. We'll work with your organization to develop a response plan that's clear and compliant. We also offer managed security services to help execute your plan. Contact us today to learn more.

CONTACT



peters & associates
simplify solve succeed