Incident Response Maturity: An Integrated Approach

An Executive Education Primer Series

Thought Leadership Matters

Incident response is not an isolated capability. It's not solved by having a series of runbooks used by your security operations center (SOC) or managed security services provider (MSSP). It's not solved by having a team of retainer-based technical experts ready to parachute in at a moment's notice to save the day. And it's not conducting tabletop exercises on an ad-hoc basis. And yet, when an organization scans the horizon looking for solutions that's exactly what it finds; a piecemeal approach being proposed by a variety of product and service providers.

Thought leadership in incident response extends well beyond a solution provider's capability to find someone, anyone who can do what's outlined in a particular statement of work. No, thought leadership is based on passion and commitment. Thought leadership actually means that someone or some people are actually thinking strategically about how to reduce cyber risk and increase organizational resilience.

At Cyber Crisis Response we have demonstrated a laser focus on cyber crisis management, however, until now we have not released our strategic framework for incident response maturity. You will not find this level of vision anywhere. This is truly what we consider *thought leadership*.

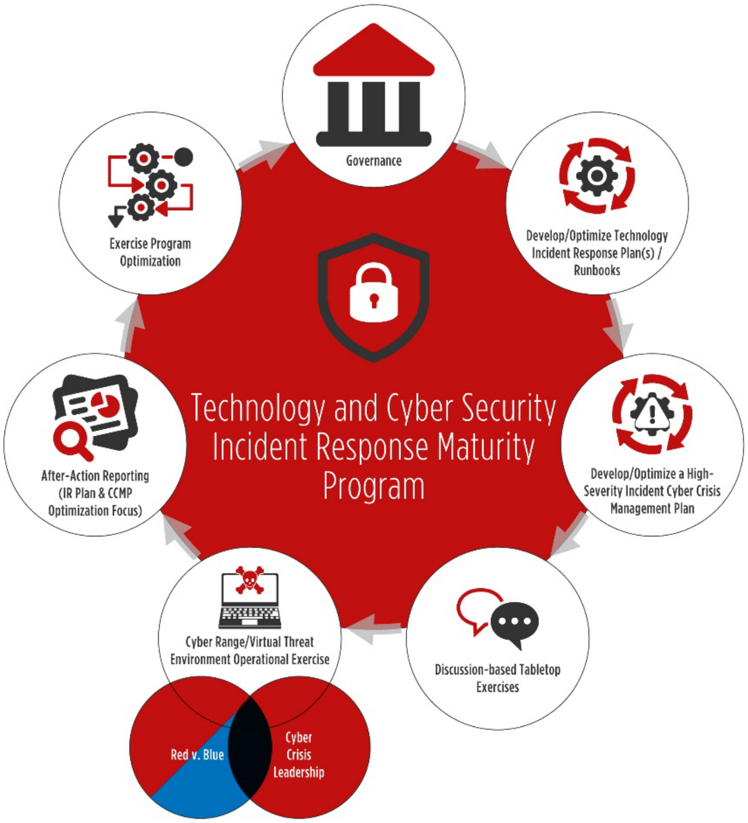
Regulatory Alignment

Let's start with the name of the solution: Technology and Cyber Security Incident Response Maturity Program. Originally, we started with Cyber Crisis Management Maturity Program but based on experience working with financial services institutions in the U.S., Canada, India, Mexico, and China in particular, we knew that financial regulators are increasingly demanding awareness and notification for incidents that are not just cyberattacks but are also operational risk events. As such, we expanded the name to include technology as a general risk source.

It's worth noting that each of the seven steps or phases are directly aligned to financial regulators, which is the core industry we have worked within. We expect that since financial and banking services are considered part of a nation's critical infrastructure, other industry regulators would have similar requirements. If not, the beauty of our model is that it is a framework designed to be flexible without sacrificing reliability and reusability.

Let's take Canada as an example. In Canada, the Office of the Superintendent of Financial Institutions (OSFI) is an independent agency of the Government of Canada reporting to the Minister of Finance that regulates and supervises domestic banks and foreign banks operating in Canada.

OSFI issued the Technology and Cyber Security Incident Response Advisory, which states federally regulated financial institutions (FRFIs) must address technology and cyber security incidents in a timely and effective manner, that policies and procedures for dealing with such incidents relating to their operations should include timely notification of OSFI, and that FRFIs should define incident materiality in their incident management framework.


Governance
Develop/Optimize Technology Incident Response Plan(s) / Runbooks
Develop/Optimize a High-Severity Incident Cyber Crisis Management Plan
Discussion-based Tabletop Exercises
Cyber Range/Virtual Threat Environment Operational Exercise
Red v. Blue
Cyber Crisis Leadership
After-Action Reporting (IR Plan & CCMP Optimization Focus)
Exercise Program Optimization
Technology and Cyber Security Incident Response Maturity Program

On the surface this may seem simplistic, however, as is common for many control requirements, they must be deconstructed to truly understand the depth and breadth of what is required. The framework referenced is linked to the Cyber Security Self-Assessment Guidance (OSFI's expectations for an incident management framework). It's in this guidance where things get far more complex. However, the reason for calling this out is to set the stage for how regulatory requirements often are more demanding than what may be on the surface. OSFI is simply one example. We have seen similar cases across the globe as regulators and central banks become much more invested in managing systemic risk.

Each of the steps or phases in our maturity program has a service description and deliverables. Of course, this is the case if we were doing the work. If you're tackling this yourself then simply use this as guidance for activities and outcomes.

Maturity Phases

Phase 1: Governance

Description:

Work with the client to assess current incident management framework and policies and identify areas for improvement based on regulatory requirements and industry best practices. One or more new policies will be developed, if none exist.

Deliverables:

- Assess existing incident management framework and related policies
- Optimize existing framework and policies, if appropriate
- Develop new framework and policies, if appropriate

Phase 2: Develop/Optimize Technology Incident Response Plan(s)/Runbooks

Description:

One or more incident response plans or technical runbooks are developed to be used by the information technology staff, most often the security operations center (SOC) or outsourced managed security service provider (MSSP), to detail the instructions to respond to, and recover from, data- and non-data related security incidents and operational risk events.

Deliverables:

- Develop technology incident response plan(s)/runbook(s) to address commodity and targeted cyber threats.

Phase 3: Develop/Optimize High-Severity Incident Cyber Crisis Management Plan

Description:

Develop a cross-organizational, cross-functional cyber crisis management plan (CCMP) designed to reduce cyber risk and increase organizational resilience. A myriad of supporting materials are required to support this "plan of plans".

Deliverables:

- Develop a cyber crisis management plan
- Train and certify key resources on effective cyber crisis management planning
  - Cyber Crisis Management Planning Professional Certification Course (C2MP2)
- Develop multiple functional incident response plans
- Develop supporting training materials
- Develop quick reference cards for key roles (CCET, CCMT, CCRT, and LIH)

Phase 4: Discussion-based Tabletop Exercises

Description:

Exercises are a key component of organizational, and national, preparedness — they provide the whole organization and supply chain with the opportunity to shape planning, assess and validate capabilities, and address areas for improvement.

Deliverables:

- Train and certify key resources on effective cyber crisis leadership
  - Cyber Crisis Management Leadership Professional Certification Course (C2MLP)
- Develop a discussion-based tabletop exercise with a subset of the CCMP representation
- Train and certify key resources on effective cyber exercise planning
  - Cyber Crisis Management Exercise Professional Certification Course (C2MEP)
- Execute discussion-based tabletop exercises

Phase 5: Cyber Range/Virtual Threat Environment Operational Exercises

Description:

Operations-based exercises include functional exercises and full-scale exercises. Operations-based exercises include a real-time response such as initiating communications or mobilizing personnel and resources. We create two aspects at this stage of the maturity process: the virtual threat environment where cyber defenders face off against threat actors in a simulated environment and a cyber crisis war room where crisis leaders are challenged to lead the organizational response to the major attack.

Deliverables:

- Develop an integrated operational exercise
- Develop a virtual threat environment that mirrors the customer's real technology environment
- Lead the integrated cyber crisis management exercise

Phase 6: After-Action Reporting (IR Plan and CCMP Focus)

Description:

A key component of an exercise is to ensure gaps in incident response and cyber crisis management plans are identified, assigned to responsible parties, and added to the governance function for monitoring to closure. After-Action Reporting is the tool for capturing the results of each exercise and the opportunities for excellence.

Deliverables:

- Develop an After-Action Report for the discussion-based tabletop exercise
- Develop an After-Action Report for the operations-based integrated exercise

Phase 7: Exercise Program Optimization

Description:

Continuous process improvement is a cornerstone for any mature and effective exercise program. At this stage of the process, the exercise team and its leadership are tasked with identifying areas of improvement and planning enhancements.

Deliverables:

- Exercise program review
- Exercise improvement planning

The corrective actions identified in phases 6 and 7 are then rolled into the Governance function where responsibility and accountability for closure are tracked.

Summary

Cyber Crisis Response, a service of Cyber Security Training and Consulting LLC is poised as a thought leader in the field of cyber crisis management. Our book, *Cyber Crisis Management Planning: How to reduce cyber risk and increase organizational resilience* provides a prescriptive, step-by-step approach to developing a CCMP. Our research-backed innovative and unique services are designed to help organizations and its leaders prepare for a major cyber incident.