BD&P LAW FIRM

What Is an Incident Response Plan and Why Every Business Should Have One

By John Sanche, Mardi McNaughton & Peter Ciechanowski

Cyber threats continue to rise in frequency and sophistication. Cyber incidents can be costly, damage an organization's reputation, and create significant stress for employees and leadership, as well as the organization's suppliers and customers. In those moments, the last thing any company wants is uncertainty about what to do.

Increasingly, industry experts have noted a gap between Information Technology (**IT**) teams and Operational Technology (**OT**) teams (i.e., those responsible for systems such as industrial control equipment). OT assets are more likely to rely on legacy technology that lacks modern security measures and, as a result, are a growing target for cyber threats. As OT-related cyber threats continue to increase, many organizations find themselves even less prepared to address these risks than those associated with traditional IT environments. Fostering stronger internal collaboration, especially between IT and OT functions, enables a more integrated understanding of organizational risk and prevents security issues from being assessed in isolation.

An Incident Response Plan (**IRP**) is a document that outlines the steps a company will take to identify, respond to, and recover from a cyber incident. Its purpose is to ensure the organization can act quickly, effectively, and consistently to avoid or minimize harm and restore operations.

Although no IRP can anticipate every possible scenario, an effective IRP provides a structured framework to be followed during a cyber incident. Proactive planning is one of the most valuable tools an organization of any size can employ.

Below are four key reasons every organization should consider implementing an IRP.

1. Establishes a Framework for Preparedness and Accountability

A strong IRP begins with a clear understanding of the organization's own environment. The first critical step is conducting a thorough internal assessment of the organization's systems, applications, networks, and operational technologies. This process goes beyond cataloguing IT and OT infrastructure; it requires organizations to look at both IT and OT environments to understand where vulnerabilities may exist and how different systems interact that create potential risks.

While many people instinctively associate cybersecurity with traditional IT measures (like strong passwords or multi-factor authentication), OT environments present their own, often overlooked, exposure points. Small and midsized organizations, in particular, may rely on a patchwork of aging equipment, legacy systems, and technologies that were never designed to communicate securely with one another. These fragmented environments can create blind spots that attackers are increasingly adept at exploiting.

An illustrative OT incident occurred in October 2025, when the Canadian Centre for Cyber Security (**CCCS**) reported that an Automated Tank Gauge at a Canadian oil and gas company had been manipulated and triggered false alarms. Following the incident, the CCCS urged organizations to "conduct a comprehensive inventory of all internet-accessible [industrial control system] devices and assess their necessity".[1] This example underscores how easily overlooked OT assets can be exploited when organizations lack full visibility into their operational environments.

By committing to this foundational work, an organization establishes a framework for preparedness and accountability. It ensures that vulnerabilities are identified before they are exploited, critical assets are known and prioritized, and decision-makers have the situational awareness needed to respond swiftly and effectively when an incident occurs.

2. Defines Clear Roles and Communication Pathways

In the midst of a cyber incident, clarity and speed are essential. An effective IRP establishes a dedicated Incident Response Team with clearly defined roles and responsibilities. This ensures that actions are coordinated, deliberate, and aligned with the organization's broader response strategy.

A well-constructed IRP typically identifies key roles such as:

- **Incident Response Lead**, responsible for overall coordination and decision-making;
- **Training Coordinator**, who ensures team members understand their responsibilities and are adequately prepared;
- **Communications Coordinator**, tasked with managing internal updates and external messaging;
- **Legal Advisor or breach coach**, who provides guidance while navigating a cyber incident, maintains privilege, and advises on reporting obligations and potential liability; and
- **IT/OT Lead**, who oversees technical triage, containment, and system restoration efforts.

[1] Canadian Centre for Cyber Security, **"Internet-accessible industrial control systems (ICS) abused by hacktivists"**, Alert AL25-016 (29 October 2025), online: Government of Canada <https://www.cyber.gc.ca/en/alerts-advisories/al25-016-internet-accessible-industrial-control-systems-ics-abused-hacktivists>.

Depending on the nature and scale of an incident, the IRP may also designate trusted external partners, such as cybersecurity forensics firms, law enforcement contacts, ransom negotiators, and/or crisis communications specialists, who can be engaged immediately without delays caused by procurement or internal approval processes.

A strong IRP not only lists these roles but also documents the individuals assigned to each one, along with current contact information, escalation procedures, and backup personnel. This level of detail ensures that communication flows efficiently and consistently, reducing the likelihood of missteps, duplicated efforts, or missed obligations.

3. Provides Assurance to Shareholders and Stakeholders

Stakeholders place significant value on governance and preparedness. An organization that has a documented and regularly tested IRP demonstrates its commitment to risk management and responsible leadership.

The consequences of failing to follow an IRP (or failing to have one at all) can be severe. A widely cited example is the 2016 Uber data breach, where hackers accessed sensitive information affecting approximately 57 million users. Although Uber had an IRP in place, senior leadership chose to bypass it, opting instead to pay the attackers to conceal the breach. When the incident eventually became public more than a year later, the fallout was significant: executives were terminated, federal criminal charges were laid, and the company faced reputational damage and regulatory scrutiny. The case remains a powerful reminder that an IRP is only effective if it is both implemented and adhered to.

Organizations that regularly review, update, and test their IRP demonstrate to shareholders, regulators, and business partners that they are prepared to respond decisively when faced with an incident. This ongoing diligence provides stakeholders with confidence that the organization can manage disruption, protect sensitive information, and uphold its legal and ethical obligations, even under pressure.

4. Establishes a Sustainable, Forward-Looking Cybersecurity Process

An IRP is not a "set it and forget it" document. It is a living framework that must evolve alongside the organization’s technology, operations, and risk landscape. An effective IRP incorporates a defined testing and review cycle (often annually, but ideally more frequently for higher-risk environments) to assess whether response procedures remain effective and aligned with emerging threats. This review process allows organizations to identify procedural gaps, validate the roles and responsibilities of team members, and integrate lessons learned from real incidents, tabletop exercises, and industry developments.

Regular testing also ensures that response protocols remain practical and actionable. Untested plans can quickly become outdated as systems change, new technologies are adopted, and staff transitions occur. By revisiting and exercising the IRP on a recurring basis, organizations maintain confidence that their response capabilities reflect current infrastructure, regulatory requirements, and threat vectors.

Conclusion

Cyber incidents are not a matter of if but when. A well-designed IRP helps an organization respond quickly, reduce damage, and restore confidence across all levels of the business.

If you have questions or would like assistance developing an IRP tailored to your organization, please reach out to any member of our **Cyber team**.