WHITEPAPER

ISA CYBERSECURITY

The Six Stages of a Successful Incident Response

The complexity of modern computer systems, coupled with the sophistication and relentlessness of cyber attackers, has made cyber incidents a matter of "when", not "if". Today, companies must have an incident response procedure prepared in advance or face the substantial – potentially existential – financial and reputational risks that come with being unprepared.

There are six key stages of cyber incident response (IR) management. These stages, recognized by global organizations like NIST and SANS, should form the foundation of your IR planning.

1 PREPARATION

With the demands of day-to-day operations, it's easy to put off the investment of time and resources required to plan for a cyber incident. But waiting is a dangerous gamble as an attack could happen at any moment. Businesses are under constant siege from external criminals, but also face internal threats – whether accidental or malicious.

Basic steps to prepare for a cyber attack:

- **Develop an inventory** of your network and computer resources to give you and your team a full picture of your risk areas.
- **Train staff on security policies** and how to recognize and respond to an incident. Do your staff have an emergency contact? Should they turn their computers off or leave them on? Whom do you call for assistance? Even basic arrangements of resources, contact numbers, dos and don'ts on a reference card, will help bring order to a stressful and chaotic situation.
- **Develop a playbook** for crisis scenarios to provide structure to your responses. Of course, incident-specific, reactive steps will always need to be taken – but they should be conducted within a well-considered and organized response framework. These playbooks must be tested periodically to help establish the "muscle memory" that is so valuable during a crisis. Knowing how/where to get information and resources quickly will save valuable moments in a crisis.
- **Construct a crisis communications plan** so you can manage the message to your clients, staff, shareholders, regulators, and business partners.
- **Cyber insurance** is an option to provide resources and a financial backstop in case of a breach.
- **Consider pre-arranging** a breach coach or expert legal counsel who can act as a guide and resource in the event of an attack. Having a dedicated resource on retainer can give support and peace of mind.

2 IDENTIFICATION

The identification stage represents the processes and behaviours that are triggered when normal operations are disrupted. You should learn of the bad news first, rather than hearing about it from customers or suppliers. The cost and scarcity of qualified technical personnel, coupled with the 24x7 nature of modern business, mean that an extended team is required to monitor and identify attacks.

What processes and procedures do you have in place to alert you of an issue?

How quickly can you gather information and identify the scope and impact of an incident?

Basic steps to prepare for a cyber attack:

- **Website monitoring** can advise whether your Internet presences are operating normally.
- **Malware detection software** can be configured to alert key staff of unusual behaviour.
- **Security Information and Event Management (SIEM) solutions,** which were out of the reach of smaller businesses only a few years ago, are now available on an "as-a-service" basis from managed service providers. These solutions provide visibility and enhanced warning of problems, with enterprise functionality at an affordable price.

3 CONTAINMENT

The purpose of this stage is to limit the damage of an attack and prevent any further impact on your business or others in your supply chain. Time is of the essence here: an orderly, well-executed containment procedure can dramatically reduce the impact of a breach. Isolating the infected systems or resources will prevent the spread of an attack and reduce the recovery time.

The playbooks you developed in the preparation stage will dictate how to isolate or contain affected equipment, data sources, logs, etc. Proper containment and isolation will also assist the forensic investigation after the fact, so this stage must be executed quickly and carefully to avoid disturbing the digital footprints of the attackers.

4 ERADICATION

Today's sophisticated malware attacks make the eradication stage more important than ever before. Depending on the nature of the incident, threat neutralization may be as simple as running anti-malware repair utilities, or as drastic as wiping systems clean and reinstalling them from scratch.

Pre-planning a response to the different scenarios is essential, and will help guide your strategies for backup, archive, snapshots, and isolating production data. Simple or complex, the eradication stage is essential. If an infection is allowed to persist, or a backdoor to a system isn't closed, then the attackers will be back soon to take out your systems again.

5 RECOVERY

During the recovery stage, your systems are evaluated to ensure they have achieved the "CIA Triad" – Confidentiality, Integrity, and Availability – indicating that your data and operations have returned to normal. You cannot be truly "recovered" until you have re-established all three of these essential operating elements.

- **Confidentiality:** Sensitive data that has been entrusted to you is private and secure.
- **Integrity:** The data that is the lifeblood of your company is accurate and intact.
- **Availability:** You can get data quickly when you need it in order to run your business effectively and efficiently.

6 LESSONS LEARNED

After a cyber incident is resolved, the focus will be on getting back to business and making up for lost time and revenue. However, a thoughtful retrospective of the incident is essential. Review what went well – and what didn't go so well.

A cyber incident can be a traumatic event for any organization, but it can be particularly devastating to a smaller business that may not have the resources to withstand the loss of revenue and goodwill that can occur.

Improving your business resilience by learning from an incident and implementing changes that make you more secure going forward, can be an invaluable investment.

NO ONE LIKES TALKING ABOUT THE POSSIBILITY OF A CYBER ATTACK

But just as businesses must conduct fire drills, creating "muscle memory" and preparedness for handling a cyber incident is essential and could make a huge difference in the event of a breach. Consider these six stages when developing your own approach for incident response.

If you'd like to learn more about incident response and how you can better prepare for the inevitability of a cyber attack, contact us. We help companies of all sizes – from local business to multi-national enterprises – with a full range of cybersecurity services.

ABOUT ISA CYBERSECURITY

At ISA Cybersecurity, our mission is to help customers achieve their privacy and security goals, and to be proactive in the fight against security threats. ISA Cybersecurity is Canada's leading cybersecurity-focused solutions and services provider, with nearly **three decades of experience** delivering cybersecurity services and people you can trust.

GET IN TOUCH

1-877-591-6711

info@isacybersecurity.com

isacybersecurity.com

Toronto | Calgary | Ottawa

Head Office:
1100 - 3280 Bloor Street W
Toronto, ON M8X 2X3