By Scott Nawrocki

Managing the Cyber Storm, Making Order Out of Chaos

The gloves have come off in cyberspace: nation states, ransomware groups, and organized cyber-criminal organizations are taking sides. Industry professionals continue to see the targeting of multinational technology companies, cyber defense solutions, and trusted identity platforms. Over the past month, the LAPSUS$ data extortion group, which takes credit for recent cyber intrusions, has gone as far as taunting their victims on social media.

As the threat landscape grows more complex, recent guidance from the Cybersecurity Infrastructure Security Agency of the United States Department of Homeland Security advises companies — large and small — to be prepared to respond to disruptive cyber-attacks. The US government, through its "Shields Up" initiative, has promulgated actions designed to minimize the effects of cyber-attacks. The initiative recommends maintaining organizational preparedness, taking steps to increase the probability of early detection of suspicious network activity, and maximizing the organization's ability to recover from a destructive cyber incident.

Maintenance of a cross-disciplinary crisis response team — composed of representatives from information security, corporate security, legal, public information, business continuity, and finance business units — is the foundation for organizational preparedness. As crises know no time of day, the team must maintain a readiness posture. Response time and manner — whether physical or virtual — must be able to meet organizational needs. In order to respond to a crisis, the team must first know of it, making redundant notification systems critical in the early stages of an incident. Redundant communication channels are vital, as the primary means of notification may fail. For example, if the organization's email infrastructure is damaged in a cyber-attack, the organization may need to employ a backup method such as automated telephonic notification.

During a critical incident, information can overwhelm responders, like water gushing from a firehose. Some initial information is inaccurate and, frankly, unhelpful. Crisis managers overseeing a data breach response can easily be overcome by this deluge of information and disinformation. Typically, there is no time to strategize or develop an action plan during an incident. The companies that fare well are those that have prepared for the threat and already have a response plan that is approved by senior

management and tested prior to the incident.

While government agencies always counsel private industry to “have a plan,” they rarely provide guidance on how to develop such a plan. Plan development is part of the art of crisis management, with methodologies varying by crisis manager. Many firms have a Critical Incident Plan covering a variety of incidents, but this is often more than one hundred pages in length and, typically, no one has read it. It certainly cannot be digested under fire.

To address this problem, firms should develop a critical incident response checklist that captures all of the essential tasks necessary to respond to a cyber-attack. Time after time, the critical incident response checklist is the blueprint for mounting a response. The beauty of the checklist is its simplicity. All personnel can read it during a crisis and abide by it. This offers a profound advantage as, most of the time, members of the critical response team are not in the same room or even the same building. The checklist — one brief, easily understood document — allows the team to enact a coordinated critical incident strategy, which is the top priority in the preliminary stages of a cyber-attack.

To develop a critical incident response checklist, firms should organize crisis response actions into three phases: Immediate, Deliberate, and Resolution and capture those actions in the checklist. Successful crisis managers make order from chaos by implementing pre-determined actions during the Immediate action phase. These actions could include taking affected workstations, systems, and servers offline during a ransomware attack. Think of this as a paramedic applying a tourniquet to stop the bleeding. Seconds count during the Immediate action phase. A crisis manager who cannot act absent management approval runs the risk that a delayed response will give the threat actor time to complete the attack, for example, by encrypting the company’s servers. In that scenario, a company without adequate backups would be forced to pay a steep ransom to regain access to its data.

Communications will fail during a critical incident and this will hamper the response. During a cyber intrusion, you must assume that hackers can monitor your communications. They will insert themselves into company calls when they have access to meeting invitations. Therefore, your critical incident response checklist should identify the out-of-band communications channel that will allow you to communicate internally and with your response team.

Once the metaphorical bleeding has stopped — once you have implemented Immediate response actions and stabilized the situation — you enter the Deliberate phase. You have the opportunity to weigh your options, convene conference calls, and consider outside assistance, whether in the form of an incident response firm or outside counsel. In the planning process, you would have already identified and vetted such entities and, ideally, put them on retainer. Being in the Deliberate phase does not mean you are in the clear. It just means that you have time for deliberation and have achieved containment of the threat.

In the Resolution phase, you have eradicated the threat from your information technology architecture and put systems back online so the business begins to operate again. Now, with the incident response fresh in the mind of your personnel, is when you should conduct an after-action conference. Talk about what went right, but more importantly, talk about what went wrong and identify the gaps in your response. Such an attack may happen again, especially if you have not corrected the systems vulnerability that allowed it.

It behooves any organization with vulnerable electronically stored data, which is to say, any organization operating in the 21st century, to work with cyber professionals to develop a critical incident response checklist and an effective response to cyber incidents. Whether conducting vulnerability assessments, drafting response plans, or assisting during an actual cyber emergency, cyber security professionals prove their worth to clients every day. The time to identify specialists with decades of experience in crisis management and first-hand knowledge of the lessons learned from a vast number of global cyber incidents is before an incident occurs. Firms should find a trusted advisor who can speak beyond the “ones and zeros” of cybersecurity and translate the threat into business risk terms.

Cyber Crisis Management 101

- **Tip #1:** Develop a critical incident response checklist to address the threats of ransomware, business email compromise, insider threat, threat hunting, vendor compromise, and data exfiltration with Immediate, Deliberate, and Resolution actions. Conduct a vulnerability assessment to determine the most likely threat in your industry and the attack that would have the highest impact on your operations.
- **Tip #2:** Without the immediate implementation of pre-determined response actions, the chaos will continue. A notification tree is critical in this phase. Do not forget to keep the public information officer, operations divisions, and business continuity personnel informed of the response status.
- **Tip #3:** Maintain an incident timeline. It will serve as a repository for information and intelligence learned and memorialize the actions taken in your response.
- **Tip #4:** Avoid taking rash actions in response to a cyber-attack. When the cyber adversary is in the driver's seat, you will be under duress and will make bad decisions. Having a critical incident response checklist with a menu of vetted options can lead to a better outcome.

Contact

Scott Nawrocki
Chief Security Officer & Managing Director,
Digital Investigations & Cyber Defense
+1 212 537 5300
snawrocki@nardelloandco.com

Nardello & Co.
WE FIND OUT