Cyber First Responders

Awareness of cyber risk is increasing, but some companies may be neglecting to prepare adequate response plans that could save them millions.

By: Antony Ireland | March 27, 2018

Topics: Business Interruption | Cyber Risks

In order to minimize the financial and reputational damage from a cyber attack, it is absolutely critical businesses have a cyber incident response plan.

“Sadly not all yet do,” said David Legassick, head of life sciences, tech and cyber, CNA Hardy.

In the event of a breach, a company must be able to quickly identify and contain the problem, assess the level of impact, communicate internally and externally, and recover where possible lost data or functionality so it can resume business operations as quickly as possible. This can only be achieved with help from the right external experts and the design and practice of a well-honed internal response.

The first step a company must take, said Legassick, is to understand its cyber exposures through asset identification, classification, risk assessment and protection measures, both technological and human.

According to Raf Sanchez, international breach response manager, Beazley, cyber response plans should be flexible and applicable to a wide range of incidents, “not just a list of consecutive steps.”

They should also bring together key stakeholders and specify end goals.

Jason J. Hogg, CEO, Aon Cyber Solutions

With bad actors becoming increasingly sophisticated and often acting in groups, attack vectors can hit companies from multiple angles simultaneously, meaning a holistic approach is essential, agreed Jason J. Hogg, CEO, Aon Cyber Solutions.

“Collaboration is key — you have to take silos down and work in a cross-functional manner.”

This means assembling a response team including individuals from IT, legal, operations, risk management, HR, finance and the board — each of whom must be well drilled in their responsibilities in the event of a breach.

“You can’t pick your players on the day of the game,” said Hogg. “Response times are critical, so speed and timing are of the essence. You should also have a very clear communication plan to keep the CEO and board of directors informed of recommended courses of action and timing expectations.”

People on the incident response team must have sufficient technical skills and access to critical third parties to be able to

take decisions and move to contain incidents fast, and knowledge of their company's data and network topology is key, said Legassick.

"Perhaps most important of all," he added, "is to capture in detail how, when, where and why an incident occurred so there is a feedback loop that ensures each threat makes the cyber defense stronger."

Cyber insurance can play a key role by providing a range of experts such as forensic analysts to help manage a cyber breach quickly and effectively (as well as PR and legal help). However, the learning process should begin before a breach occurs.

Practice Makes Perfect

"Any incident response plan is only as strong as the practice that goes into it," explained Mike Peters, vice president, IT, RIMS — who also conducts stress testing through his firm Sentinel Cyber Defense Advisors.

Unless companies have an ethical hacker or certified information security officer on board who can conduct sophisticated simulated attacks, Peters recommended they hire third party experts to test their networks for weaknesses, remediate these issues and retest again for vulnerabilities that haven't been patched or have been newly appeared.

"You need to plan for every type of threat that's out there," he added.

"If I hear a client say it is perfect and then I look at some of the results of the responses to breaches last year,

there is a disconnect." — Rich DePiero, head of cyber, North America, Swiss Re Corporate Solutions

Hogg agreed that bringing third parties in to conduct tests brings "fresh thinking, best practice and cross-pollination of learnings from testing plans across a multitude of industries and enterprises."

Legassick added companies should test their plans at least annually, updating procedures whenever there is a significant change in business activity, technology or location.

"As companies expand, cyber security is not always front of mind, but new operations and territories all expose a company to new risks."

For smaller companies that might not have the resources or the expertise to develop an internal cyber response plan from whole cloth, some carriers offer their own cyber risk resources online. Evan Fenaroli, an underwriting product manager with the Philadelphia Insurance Companies (PHLY), said his company hosts an eRiskHub®, which gives PHLY clients a place to start looking for cyber event response answers.

That includes access to a pool of attorneys who can guide company executives in creating a plan.

"It's something at the highest level that needs to be a priority," Fenaroli said. For those just getting started, Fenaroli provided a checklist for consideration:

- Purchase cyber insurance, read the policy and understand its notice requirements.

- Work with an attorney to develop a cyber event response plan that you can customize to your business.
- Identify stakeholders within the company who will own the plan and its execution.
- Find outside forensics experts that the company can call in an emergency.
- Identify a public relations expert who can be called in the case of an event that could be leaked to the press or otherwise become newsworthy.

"When all of these things fall into place, the outcome is far better in that there isn't a panic," said Fenaroli, who, like others, recommends the plan be tested at least annually.

Cyber's Physical Threat

With the digital and physical worlds converging due to the rise of the Internet of Things, Hogg reminded companies: "You can't just test in the virtual world — testing physical end-point security is critical, too."

David Legassick, head of life sciences, tech and cyber, CNA Hardy

How that testing is communicated to underwriters should also be a key focus, said Rich DePiero, head of cyber, North America, Swiss Re Corporate Solutions.

Don't just report on what went well; it's far more believable for an underwriter to hear what didn't go well, he said.

"If I hear a client say it is perfect and then I look at some of the results of the responses to breaches last year, there is a disconnect. Help us understand what you learned and what you worked out. You want things to fail during these incident response tests, because that is how we learn," he explained.

"Bringing in these outside firms, detailing what they learned and defining roles and responsibilities in the event of an incident is really the best practice, and we are seeing more and more companies do that."

Support from the Board

Good cyber protection is built around a combination of process, technology, learning and people. While not every cyber incident needs to be reported to the board room, senior management has a key role in creating a culture of planning and risk awareness.

"Cyber is a boardroom risk. If it is not taken seriously at boardroom level, you are more than likely to suffer a network breach," Legassick said.

However, getting board buy-in or buy-in from the C-suites is not always easy.

“C-suite executives often put off testing crisis plans as they get in the way of the day-job. The irony here is obvious given how disruptive an incident can be,” said Sanchez. “The C-suite must demonstrate its support for incident response planning and that it expects staff at all levels of the organization play their part in recovering from serious incidents.”

“Cyber is a boardroom risk. If it is not taken seriously at boardroom level, you are more than likely to suffer a network breach.” — David Legassick, head of life sciences, tech and cyber, CNA Hardy

“What these people need from the board is support,” said Jill Salmon, New York-based vice president, head of cyber/tech/MPL, Berkshire Hathaway Specialty Insurance.

“I don’t know that the information security folks are looking for direction from the board as much as they are looking for support from a resources standpoint and a visibility standpoint. They’ve got to be aware of what they need and they need to have the money to be able to build it up to that level,” she said.

Without that support, according to Legassick, failure to empower and encourage the IT team to manage cyber threats holistically through integration with the rest of the organization, particularly risk managers, becomes a common mistake. He also warned that “blame culture” can prevent staff from escalating problems to management in a timely manner.

Collaboration and Communication

Given that cyber incident response truly is a team effort, it is therefore essential a culture of collaboration, preparation and practice is embedded from the top down.

One of the biggest tripping points for companies — and an area that has done the most damage from a reputational perspective — is in how quickly and effectively the company communicates to the public in the aftermath of a cyber event.

Salmon said of all the cyber incident response plans she has seen, the companies that have impressed her most are those that have written mock press releases and rehearsed how they are going to respond to the media in the aftermath of an event.

“We have seen so many companies trip up in that regard,” she said. “There have been examples of companies taking too long and then not explaining why it took them so long. It’s like any other crisis — the way that you are communicating it to the public is really important.”

With additional reporting by Dan Reynolds, editor-in-chief of Risk & Insurance.

Antony Ireland is a London-based financial journalist. He can be reached at riskletters@lrp.com.