How organisations should respond to cybersecurity incidents?

09/11/2017

Information Law analysis: David Cass, chief information security officer at IBM, and Daniel Garrie, senior managing partner at Law and Forensics, explain the steps organisations should take in case of a cybersecurity attack.

What should companies be doing to ensure their systems and processes are well prepared to withstand a cybersecurity breach, and how can they assess and manage potential vulnerabilities?

Preparation is the key to successful incident response—while remembering that nothing ever goes according to plan.

During the past two years we have seen cyber-attacks escalate from theft of information to crippling an organisation's ability to conduct business. It is evident that cyber threats are a material risk to an organisation and not just a technology risk. This means that the entire organisation must participate in incident response planning. Although in practice nothing goes quite according to plan, companies taking a holistic approach are certainly going to be in a better position when dealing with a cyber incident.

Lawyers must realise that the entire business must be involved in the preparation with representation from executive management, business operations, legal, communications (both internal and external), IT, and information security.

Once you have this team assembled, take some time to establish roles (these evolve over time), and identify the assets and areas of operation that will be most appealing to a cyber attacker. From intellectual property to financial information to healthcare information, no matter what industry you are in, if you are doing business, you have something that someone wants.

Utilising a cross functional team to identify types of information is critical, as what one division deems important to operations may be overlooked by another team that does not utilise that information.

Remember the old adage: one person's garbage may be another's gold—data which seemingly has little or no value to a company may be of great value to hackers and put data subjects and the company's business or brand at risk if compromised. Identifying these potential targets, while also determining each team member's role in planning are important first steps.

Roles and responsibilities

Generally, executive management is responsible for making major operational decisions that may arise as a result of the incident while the business operations team will offer guidance on choices regarding ongoing activities.

The legal department plays a vital role, as different types of incidents have the potential for significant consequences and fines for organisations. For example, applicable laws may require regulators or other persons to be notified of the incident.

By identifying the types of information you have, each of the categories may require a different response. In addition, the legal team should identify what outside counsel they may want to bring in for additional guidance during the planning period.

The communications team needs to develop plans on keeping employees informed of what is going on and keeping customers informed of what happened, what steps the organisation is taking to remediate the issue and any potential impact to them.

Keeping employees informed, includes giving them guidance on how to respond to customer calls, who they should refer people to for comment in the event the press is calling them, and how they can help continue operations.

The IT department needs to be engaged in order to restore impacted services or systems, and work with information security to limit the potential spread of the attack. Information security will be working across the teams to identify impacted systems, look for signs of exfiltration, capture forensic evidence just to name a few of the activates.

Once these teams are brought together, the group can start to build response plans based on different scenarios, such as exfiltration of customers' personal data or a disabling ransomware attack. These are only a small subset of examples, but each scenario requires a different response.

Incident response planning

The next step is to map out incident response plans. If your company is hit with ransomware, how will you communicate to employees and customers, do you have the capability to restore the systems without paying and how long will it take to be operational and how will you interact with law enforcement?

Once these plans or runbooks are made organisations must regularly practice responding to them. The practice may be quarterly, twice a year or even once a year depending on what type of business you are in.

Practice sessions can be as simple as assembling the above team and talking through the different scenarios or large scale 'table top drills'. But practice is the key to preparation. Organisations that develop plans and never test or practice them, perform only marginally better than organisations without a plan. When the event is occurring, you want familiarity with the plan and will have learned countless lessons from table top exercises which will lead to a much more organised and cohesive response.

Preparation should also include knowing and working with your regulators whenever possible. The first time you are meeting with them should not be during an actual incident. The same holds true for working with law enforcement. Establish your contacts early, and learn how to work with them. This will make engaging with them during an actual event work more effectively and efficiently.

There are too many scenarios to discuss in a brief synopsis, so let's take the following example:

An employee just returned to the office after working remotely. He accidentally clicked on a malicious file that encrypted his laptop. He connects to the network, and proceeds to call the help desk, thinking they can help him reset or decrypt his laptop. While connected to the company network, the ransomware starts to propagate across the network and the information security department starts to see alerts on their security, security information and event management (SEIM) systems.

In an ideal scenario, they recognise the alerts and start an immediate response based on the play books created from the integrated planning sessions. Keep in mind this type of attack spreads rapidly and if the organisation suffers from alert fatigue (where they receive more alerts than they can respond to) the spread may be significant before incident response has started.

Once a cybersecurity breach has been correctly identified, what immediate action should be taken?

Once the attack is identified, the information security team with the IT team should be trying to limit the spread, which should include getting the infected devices off the network immediately, taking specific actions to quarantine the spread, such as isolating network segments (all of which have the potential to impact operations). The IT team should be looking at the backups and their status for a potential restoration of systems. Often these attacks also include exfiltration of sensitive data, so you may have legal obligations and determining what has been exfiltrated may take time.

Key priorities at this time include limiting the spread, protecting ongoing operations, and identifying types of data that may have been exfiltrated. Evidence needs to be collected and the person or team that is authorised to contact law enforcement actively engaged. The person or the team for this should have been identified as part of the planning exercise above. If you have made the decision to engage law enforcement, the process for gathering and preparing evidence should be part of the information security team's playbook already as this often requires certain tools and techniques that could be an article unto itself.

In the ideal situation the organisation would be able to limit the spread, restore services, and limit the exfiltration of data. As seen through recent attacks in the news, this optimal scenario frequently does not occur, so let's examine the worst case scenario. The ransomware spread throughout the organisation and has encrypted key systems, employee laptops and your network attached back up system. Now what? Do you pay the ransom, do you have offline backups that you can restore from (how old are they and when were they tested for restoration last)?

How long will it take to restore the systems if you can? This is often measured in weeks not hours, depending how widespread the impact was. How do you communicate with employees and the outside world and what does it take to ensure you can continue operations.

Recent attacks indicated that several impacted organisations had to pay the ransom either because they did not have adequate backups or they could not incur several weeks' of disruption while restoring from backups. However, there have been several organisations that paid ransoms and were subsequently still unable to decrypt their data. In addition, once you pay you possibly position yourself as a target for more ransomware attacks. However, this highlights why preparation and follow through are so important. Having a plan to restore from backups—and most important, following through on the plan—will limit impact and make for a smoother response.

How should companies follow up a cybersecurity breach?

This brings us to the post incident review. This part of the process is critical, as even with appropriate plans in place there is never a perfect response and organisations will always have something to learn. These reviews must be more than a get together and review—there must be takeaways and actions that can be followed up on.

Going back to our example above, part of the review should include how the ransomeware spread across the environment so quickly, and where did it originate—eg an employee, system or maybe a third party vendor who had access to systems for maintenance.

The rapid spread may have happened as a result of the organisation’s network being flat, which means it was lacking adequate means of segregation and separation of different environments. This could have occurred by flawed design or maybe the company has grown over time through acquisitions and added to the environment, unknowingly increasing the potential exposure. In this case that information should be part of the post incident review process with actions to be taken.

As we’ve seen in recent attacks, communication is key to trust and brand reputation following an incident. Were you able to communicate with employees via text during the outage? Did it work? What did not? Was the incident announced publicly? What additional communication is needed? Did you follow the priorities identified during planning and in the order the organisation agreed upon such as limiting/containing data exfiltration, quarantine of impacted systems, continuous operations, communications with employees and customers, engagement with law enforcement and restoration of impacted systems?

Organisations that plan, practice, use an integrated response, and learn from post incident reviews recover faster while standing the best chance at maintaining the goodwill of their customers.

Interviewed by Mervet Kagu.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.

This article was first published on Lexis®PSL Information Law on 9 November 2017.