Navigating a cyber incident: Your key stakeholders

In the dozens of cyber incident scenarios we've helped client teams to wargame using our behind-closed-doors software and roleplay service, we've identified patterns in the key stakeholders involved – as well as those overlooked by teams grappling with an incident of unknown scale and severity. We've mapped out the key groups you'll need to have lines of communication with during a cyber incident, to ensure not only that business operations are restored quickly, but that the long term outcomes for customer trust, share price and licence to operate are positive.

Customers

Those affected need clarity on the potential impact on them, their privacy and relationship with you, and what they can do to protect themselves. Those unaffected will expect business as usual, but may have questions. Be proactive in helping customers pre-empt problems and spot suspicious activity

Partners

IT operations are often inextricably linked: the incident may have affected your system, but what could the impact of eavesdropping or phishing of your users be on partners' clients or joint ventures? You'll need to keep partners informed on your customer messaging and provide regular updates on system status

Staff

Your staff may be victims of the breach too, and need similar reassurance to that you offer customers. But with their own networks and channels, it's important you're clear with them about what's known so far, what's being done and what they should and shouldn't be sharing with friends and family

IT Operations

Your IT function needs to work at pace and with creativity in a cyber incident. While you can't expect the full facts of the incident immediately, you need regular updates from a nominated point of contact, and the capability to translate technical issues into customer or staff advice

IT Forensics

You need a trusted internal or external team with the 'white hat' skills to get to grips with your infrastructure quickly, as well as establish the scope, impact and source of the issue. In the case of an insider threat, this may need to be explicitly separate from mainstream IT

Expert Commentators

A cyber incident will bring out critics and cynics, but some of the discussion online will be informed and constructive. Opening a private channel of contact with these experts may help you pick up intelligence from them more quickly

Community Advocates

Winning back the trust of your customer community is vital, so building relationships with intermediaries and leaders of key forums can give you a trusted group who can cascade your messages to their own members

Media

You'll need clear messaging and credible prepared holding lines for both consumer/trade outlets as well as more technically-minded media. Remember, reporters will be talking to customers and expert commentators too, but it's important affected customers hear from you before they read about it

Regulators

Depending on your industry and jurisdiction, you'll want to start opening a line of communication and preparing proactive notifications to regulators as soon as you have the basic facts of the incident. Missing key deadlines – 72 hrs in Europe – can mean fines

Legal & Insurance

Involve legal colleagues early and check the terms of insurance policies. If you're held to ransom or threatened with a class action you'll need to move quickly and ensure your actions don't cause liability issues; likewise, involving lawyers early may help ensure that timely communication with customers isn't delayed

Human Resources

In the case of an insider threat, you'll need to review staff screening, access and usage logs and potentially suspend internal systems. HR need to be ready to support an investigation and also help with staff communication to guide worried employees about what to do and say

Suppliers

Often overlooked, your supply chain is both a source of potential vulnerability and also a crucial partner in handling an incident well. You need out-of-hours contacts and emergency support in place in case of incidents and to ensure that suppliers can complete their own investigations quickly and report back to you

Law Enforcement

Tread carefully: involve law enforcement and cyber agencies too early and you may find your room for manoeuvre constrained, e.g. in a ransomware situation. But in parallel with your investigation and any legal or insurance action, you may need to report the incident, and specialist agencies can provide useful support

Investors

Cyber incidents can trigger serious share price falls but when handled well, the long term effects are minor. Keeping a line of communication with investors can provide reassurance that you have control of the situation and are involving the right stakeholders to minimize regulatory trouble

social simulator