ISTARI Perspectives

Cyber crisis preparedness: How to craft a winning playbook

Jo De Vliegher
Andy France OBE

Interview by
Dr. Manuel Hepfer

10 • 2022

"Being prepared for cyber crises can help improve general crisis preparedness and vice versa."

Jo De Vliegher
Client Partner at ISTARI and former CIO at Norsk Hydro

Organisations deal with crises differently. In some, chaos and disorder sprawl, whereas others seem to operate out of an in-built calmness that enables them to rise to the challenges presented.

No organisation that suffers a serious cyberattack can rely on the hope that its people will just cope. Instead, it needs a playbook and routines to stress test that.

When global aluminium producer Norsk Hydro was hit by a ransomware attack that disabled 22,000 computers across 170 sites in 40 countries, leaving its 35,000-employee workforce relying on pen and paper, it gained valuable lessons on how to prepare for future cyber crises (the BBC reported on the attack).

In this interview, Jo De Vliegher, former CIO at Norsk Hydro and now a client partner at ISTARI, shares what he learned about preparedness and resilience. Joining him for this discussion is Andy France, co-founder and director at Prevalent AI and former deputy director at GCHQ, the U.K.'s intelligence and security agency, who has observed and advised dozens of companies on cyber resilience and responses.

Manuel Hepfer, a cybersecurity researcher at ISTARI and Oxford University, interviewed both executives. What follows is an edited version of their conversation.

Manuel: Jo, having been the CIO at Norsk Hydro when the cyberattack hit, how do you approach cyber crises now?

Jo: Let's first define our terms. I think of these in three levels. A cyber "event" is when you detect an anomaly in your system, which may not even have been caused with malicious intent. Next comes a cyber "incident," which has malicious intent but can be dealt with through normal day-to-day operations. I define a "crisis" as that moment when normal mandates, processes and hierarchies are insufficient to contain the damage and it is impossible to go right back to business as normal.

What you do to prepare for any crisis makes the difference between surviving and getting into serious trouble. The first step in preparedness is making people understand what a crisis really means. People's tendency to underestimate considerably how bad a crisis can be is, in my opinion, one of the biggest inhibitors of proper preparedness and resilience. If you are training for the Olympic Games but you think that this will be no different to a local sports race, you will fail.

Cyber crisis preparedness is an offshoot to general crisis preparedness. It is different from general crisis preparedness in two ways: First, a cyber crisis involves an active adversary – someone purposefully trying to cause damage. That means that unlike, for example, a fire or flood, a cyberattack is not an isolated, accidental incident. It can involve interactive periods in which you have to think about the attackers' potential next move.

Second, cyber crises typically hit a company more broadly. A fire or flood typically affects a single geography or department. A cyberattack by contrast can hit all departments globally within minutes, even seconds. Not many other crises have that same immediate extent of impact. So, in your cyber crisis preparedness, you need to account for that.

In my experience, being prepared for cyber crises can help improve general crisis preparedness as well and vice versa.

Manuel: From having observed dozens of companies responding to serious cyberattacks, Andy, what are the common challenges you see?

Andy: Businesses often struggle to prepare and respond because they think of a cyber incident as a linear thing; if you crash a car, it tends to produce similar kinds of damages.

But in cyber, the same actor and the same malware in one company might have a completely different impact in another company in the same industry. I'm really thinking about ransomware here because of how it gives rise to operational, reputational or financial stress.

The other mistake is to think, "We've already got a plan in place. It's called the business continuity plan." But a business continuity plan and a cyber crisis response plan are not the same. If you take out your business continuity plan and try to use only that to respond to a cyber incident, you'll probably make progress for no more than half an hour. There is some degree of overlap, such as the availability and restoration of systems, but a business continuity plan won't have factored in data theft and dealing with a criminal gang intent on extortion.

Manuel: Norsk Hydro faced multiple weeks of system downtime with varying degrees of severity. How did your response evolve?

Jo: I now look back and think about the need for two kinds of preparation: preparing for immediate, short-term support and preparing for rebuilding for the future. Immediate support allows you to continue communicating, to keep business operations running and to get external help early. Those are important in the first hours and days of a crisis.

The other element is to prepare for rebuilding and recovering for the future as safely and quickly as possible. One thing we learnt at Hydro: You cannot have the same people trying to fix systems at the same time that you need them for critical operations while the attack is still ongoing. These have to be separate teams. With the right process, you have an opportunity to build back better – to emerge stronger with less legacy, deficiencies and weaknesses.

Companies should ask themselves: How do we prepare for different phases of a crisis? How long can we survive in each mode? When should we go to the next mode? And what happens if that is not yet possible?

Manuel: Is there a downside to planning, Andy? Can companies prepare and plan too much?

Andy: You don't need a plan that defines everything in perfect detail. You don't play a football game deciding in advance who's going to be where exactly in the 63rd minute on the pitch. Instead, you have an overarching set of objectives about how you want to play, but you are cognisant that it's a dynamic game. Those companies that have done really well in an existential crisis had a playbook. That playbook clearly laid out roles and responsibilities, layers of authorities and processes that kicked in in the wake of a crisis. That playbook also needs to say which assets are most important. Whether that's data or production facilities doesn't matter but it needs to include who's responsible for which asset.

Manuel: Jo, how can a company know in advance if they are ready for a crisis or not? How can they test their preparedness?

Jo: It starts, as Andy says, with having identified the company's crown jewels – assets, business processes, reputation – and thinking through how those will be impacted in different credible scenarios. These scenarios must be detailed, relevant and plausible. A ransomware attack is an obvious scenario but it shouldn't be the only one. Without suitable scenarios, the rest can't follow.

The second thing that has to be in place are playbooks of how the organisation is planning to respond. And the third step is ensuring that critical roles are allocated to the right people, internally and externally.

Finally, companies need to make sure these playbooks have been practised. Tests, fire drills or purple teams are not only indicators of preparedness but also sources for continuous improvement.

Manuel: What does a good practice session look like to you, Andy?

Andy: Cyber preparedness is a discipline that plays out over different levels and different personas play different roles.

Take the board, for example: It would be an overkill to run a scenario at every board meeting but perhaps one board meeting every six months. At the edges of the board meeting, you sit down and go, "We're just going to walk through this scenario. This is what could happen. It's an exercise."

But as Jo said, these exercises need to be plausible and specific. Many consultancies tend to come in and say, "The sky is falling, the world is ending, and your business is almost dead." Executives tend to react dismissively and argue that this isn't going to happen to them. They then take themselves out of the discussion, which isn't helpful. Any practice scenario has to be based on reality – grounded in what the business does and how it operates. You don't have to address every issue in one scenario. The more you practice, the easier it becomes to respond effectively should you have to do it for real.

Manuel: Jo, who should be in the driver's seat in preparing for cyber crises?

Jo: Cybersecurity risk is a business risk that is triggered by a digital event. As such, cyber crisis preparedness should reside

as high as the board and the executive management but IT and cybersecurity professionals can be responsible for spearheading the effort and creating the scenarios that are the start of an impact analysis. This should not just be cybersecurity people having to imagine the business impact. It is more about sitting together with the business owners and finding out what the true impact for the company could be.

I was recently helping a company improve their preparedness and asked them what they will do when their manufacturing plant is attacked. They said, "I would first go to my plant control centre and check the impact." But if the control centre is unavailable, what do you do? Doing that deep dive is when business and operational people truly understand the impact of a crisis: If the support systems that you rely on in other crises are gone, what do you do?

Overall, effective crisis preparedness is about building a capability for minimising the consequences of an attack and for getting back to business as usual as quickly as possible. Those companies that are prepared will have a big advantage following a cyber crisis.

About the authors:

Jo De Vliegher

Formerly the CIO at Norsk Hydro, Jo is a client partner at ISTARI. He is a globally recognised authority in crisis management, advising companies on cyber resilience, crisis preparedness, and crisis response. He is a frequent keynote speaker at leading conferences and has appeared in media outlets, such as The Wall Street Journal.

Andy France OBE

Formerly the deputy director (cyber defence) at GCHQ, Andy is co-founder & director at Prevalent AI and managing director at RedQ Ltd. He helps and advises large companies on improving their cybersecurity programmes.