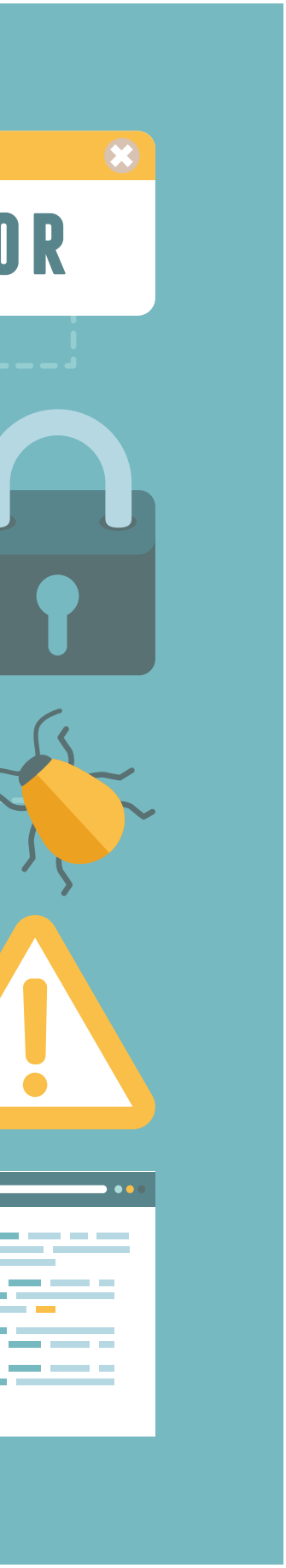
Help us choose our Top 10 Topics for 2018
www.deloitte.com/lu/InsideRisk2018h



Fight fire with fire

Cyber response training through immersive simulation

Dominic Cockram
Partner
Deloitte UK

Making sure you have an effective management response to cyber crises is a key requirement for any 21st century business. But how can you optimize your cyber response capability? Simulating a crisis is one way to see just how ready you are—or how far you have to go!

In this article, we consider the unique challenges presented by a cyber-related crisis, setting out the options for building up your cyber response capability and preparing your cyber response teams to perform optimally to protect the reputation of your business and minimize losses.

Effective cyber crisis management is dependent on having the right people in the right roles, with good, well-understood procedures and processes, supporting tools, and effective leadership.

A crisis, by definition, is a situation that poses a serious threat to an organization and requires decisive action at a strategic level to minimize the impact on the business and its stakeholders. The stakes are high, and all crises create a complex, stressful, and high-pressure environment for those involved. The “cyber factor” brings added nuances and an uncomfortable interface between the complex IT domain and strategic decision-makers. Add to that social media, journalistic and regulatory scrutiny, and public opprobrium and you have the perfect ingredients for a nightmare scenario.

So, what characterizes a cyber crisis?

Speed
They usually hit businesses fast and without warning. The very nature of technology means issues move and spread quickly.

Complexity
They are usually the result of an attack on you or your systems and, as with most planned assaults, they are designed to make matters opaque, confusing, and chaotic to enhance the attackers' opportunities to achieve their objectives.

Uncertainty and lack of (or sometimes too much) information
Uncertainty is a characteristic of all crises but with a data breach or a ransomware attack, this is often magnified by an initial lack of understanding of what has happened. With floods and fires, the nature of the disaster is clear; with malware or breaches, you may never know what happened.

Terminology and technical awareness
While awareness is growing, there is still a significant gap in understanding between the technical IT experts and the strategic decision-makers in a company.

Victim versus villain
You may feel like the victim, but to many, the external perception may be that you are the villain. If customer data has been lost or systems paralyzed, people may begin to ask why you "allowed" this to happen.

Media scrutiny and public outrage
To lose sensitive personal data hits right at the heart of customer trust and will attract intense media and public scrutiny.

Timelines
To understand what has happened, why and just how bad the situation is takes time. However, time is not a luxury you have when it comes to communicating with your stakeholders.

"Wicked" decisions
will you shut down key systems, shut customers out from websites or, as a last resort, disconnect from the internet? Plenty of difficult decisions will have to be made.

What makes good cyber crisis management?

Effective cyber crisis management is largely dependent on having the right people in the right roles, with good, well-understood procedures, supporting tools, and effective leadership. However, human behavior during a crisis response is also a key factor. We can be resilient, adaptive, and flexible, but our behavioral patterns can also be plagued by error, stubbornness, and inefficiency. Therefore, the executive team must have a repertoire of effective crisis management skills to function in situations involving high levels of stress, complexity, and time pressure. Maximizing those skills depends on the level of experience with and exposure to previous events.

Readiness to respond to a cyber crisis

Building skills and widening experience would be easy if you could learn on the job and slowly build your expertise. However, crises do not happen every day, so cyber response capability must be developed, validated, and improved through an accelerated mechanism of frequent practice, training, and exercising of the people involved—particularly the leadership at each response level and the strategic executive group. Just like a football team, the more training and practice they do, the quicker they fall into their drills and patterns in a match, perform as a team, and score goals.

The right training environment for every level

Crisis training provides the ideal training environment, building people's experience through exposure to different scenarios under various conditions. The aim is to develop their muscle-memory from lessons learned so that they can be applied to real events. Many different types of exercise exist; each approach builds different capabilities and is chosen to suit the maturity of participants.

- **Cyber workshop**—introducing teams to the issues around cyber response and crisis management using case studies, videos, and scenarios to raise understanding of the issues and challenges to be faced.
- **Cyber desktop (tabletop)**—take a scenario and bring together the key cyber response teams to "walk and talk" the response against a timeline. Useful for discussion and establishment of roles and responsibilities.
- **Red teaming**—an assault on your defenses in real time during a simulated "hack" or penetration test. Great for testing your defenses and validating your monitoring of alerts and notifications. Highly operationally focused but can, on occasion, be linked to strategic decisions.
- **Cyber incident team training**—exercising your technical "quick response" team (CSIRT, CIRT, etc.) and their ability to use their tools, assess and analyze the data, conduct a coherent and coordinated investigation and sleuth their way to the answers based on a real trail of simulated intrusion paths and clues using safe and tested methodologies playing out on your network in real time. How else can you check just how good they really are?
- **The "full" cyber simulation**—rehearsing the end-to-end response to a large-scale cyber crisis. Scenarios start with alerting and mobilizing the CIRT and the technical teams, while rehearsing the escalation up to the business/management level and then to the strategic team. Each level has to consider the issues and requirements of its remit, and the interplay of responsibilities upward and downward. Internal and external communications are also critical; bringing the media, public, investors, and other stakeholders into play, adding to the strategic challenge. The business impacts unfold, while the technical teams investigate the cause of the crisis.

For many businesses, immersive cyber simulation exercises are the most appropriate tool for building crisis response capability.

Experiential, immersive simulations

For many businesses, immersive cyber simulation exercises are the most appropriate tool for building crisis response capability. Such exercises truly test the end-to-end response, taking the teams from alert through to the most senior executives and placing them all in the maelstrom of a cyber crisis.

Perception versus reality

To rehearse a team's performance, simulations must have the ability to create the perceptions, emotions, and behaviors that occur in real crises. Therefore, any simulation should be engaging at its developmental center. For simulation exercises to be engaging they must be credible to the players. This is achieved by incorporating high levels of fidelity, complexity, dynamicity, and opaqueness in the cyber crisis scenarios used during the exercise.

Generating immersive detail

Successful simulations are immersive, with players becoming fully involved and responding as if the scenario playing out in front of them were reality. Key to generating this environment is the scenario and the detail, facts, and storylines created behind the scenario. The scenario must have the ability to adapt during the exercise in response to the decisions and actions the teams have taken. This approach requires experience and depth of planning to ensure that there is sufficient background to make changes to the scenario during the exercise.

Immersive simulations are the only tools that truly test and validate the efficacy and coherence of your cyber response capability because they re-create the reality that is faced in the early stages of a cyber crisis. Being under the pressures and desires for more information, the reaching for facts and certainty, and the wicked decision of whether to go public or not.

To play these critical points out in a simulated reality is to learn where the conflicts are, where policy fails to meet reality, and where reputation overrides logic and perception challenges fact.

The Wannacry and NotPetya attacks have established a whole new paradigm of cyber challenges to be faced and managed.

Building the right cyber challenges

Scenarios versus training benefits

Scenarios are central to any cyber simulation, but some scenarios suit teams at certain levels better than others; for example by providing more scope for technical detail or focusing on media and other stakeholder issues.

While there is, often quite, rightly a desire to test the scenarios that are highest on the risk register, at times it is better to choose the right scenario to rehearse the response capability of the teams and to provide a longer, more thorough step through of the assessment, escalation, activation, response, communication, and recovery stages of the cyber response.

Not enough hours in the day

In addition, a further challenge is that of time. There is only so much time available in the agendas of senior executives and thus exercise play is often squeezed into a single day—or even worse, a three-hour slot—which prevents certain key, longer-term decision points from being played out, such as notifying the regulator following a data breach (under GDPR within 72 hours). Such critical decision points can be neglected in a one-day exercise unless time jumps are introduced to allow the fast forwarding of events.

Post-data-breach customer engagement considerations

Under the forthcoming GDPR rules, businesses in Europe will be under far more pressure to proactively notify customers of a breach and to conduct a full "breach notification and customer engagement" program. This in itself is beginning to provide a specific scenario worthy of exercising and validating. An organization's ability to respond and manage the customer engagement with appropriate resources, messaging, and identity protection considerations are all critical considerations, as is the all-important insurance discussion.

Train hard, fight easy

"Train hard, fight easy" is a great cry of the armed forces, but very true in all arenas surrounding crises. The better prepared the response, the better we are able to deal with the chaos of a crisis and deliver well-informed decisions in a timely fashion. This article has only touched on the edges cyber crisis preparedness, and there is much that can be done to build a real capability.

Most large organizations recognize that the question is "when," not "if," they will be beset by some form of cyber crisis. The Wannacry and NotPetya attacks have established a whole new paradigm of cyber challenges to be faced and managed.

At the same time, GDPR brings to Europe—and all those businesses with customers inside Europe—new and much tougher regulations, and preparedness is one of the many facets now in focus.

Against this backdrop, it is no longer acceptable for any business not to be well prepared and rehearsed. That ability to be able to show, post any form of crisis, that you were as well prepared as you could (and should) be is invaluable in the investigations that follow.

Most critical is that your teams are genuinely trained and have experiential awareness of the different types of cyber challenge built up. This must be through simulations of just what each crisis can present in terms of key decisions, challenges, and communication nuances.

Knowing that from top to bottom your business has played through the interaction of teams at every level is the only way to really know you are ready to go out and defend your business and its reputation at its most vulnerable time.