ExpertInsights@IBV

Beyond the boom

Improving decision making in a security crisis

IBM Institute for Business Value

Coping with security crises

High-profile data breaches that affect millions of people are hitting the headlines with increasing regularity, and CEOs of large corporations are being dragged in front of government committees to be grilled by lawmakers. Harsh questions like “How could your security be so lax?” and “Why didn’t you know what happened and why did you respond so slowly?” can be a nightmare for a CEO. Most companies focus IT resources on detection and prevention and don’t pay enough attention to response and remediation.

Understanding the timeline of a breach

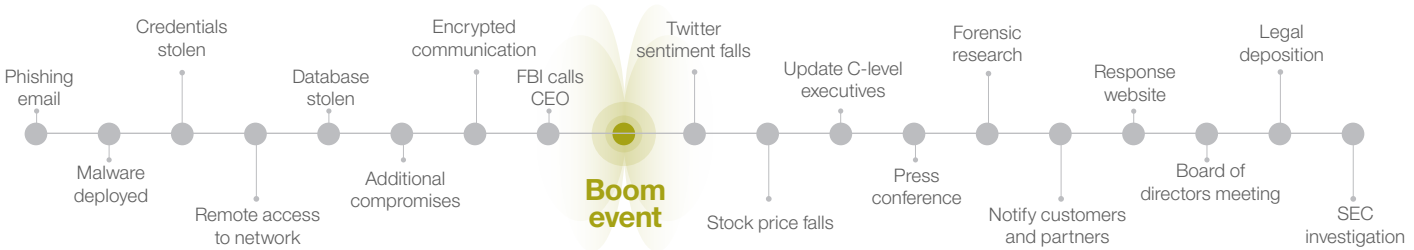
Recent high-profile security breaches highlight a lack of preparedness among many organizations. In a given 24-month period, a business has a one-in-four chance of being hit by a significant threat.[1] Yet a startling number of organizations are completely ill-equipped to handle a major security incident. In fact, a study from the Ponemon Institute found that 75 percent of organizations don't have an incident response plan applied consistently across the organization.[2] This failure is particularly alarming when you consider the fact that breach notification laws and regulations are becoming stricter around the world, with decreasing times allowed for reporting to government parties and the public.

During the lifecycle of a security breach, several critical events happen. The first event is the point when a breach occurs. The second is when data has been taken or destroyed. The third is when the breach is discovered (either by external or internal parties). And the fourth is when the breach is made public. When it comes to incident response, each of these points in the timeline are colloquially called "boom" events. However, we're assuming here that the boom event is the point when the breach hits the media and the company loses control of the story (see Figure 1).

Although the news media often focuses on the event itself, breaches often span many months. Before the breach is disclosed or discovered is termed the "left of boom." During this time, cyber thieves are taking credentials, gaining deeper access, stealing data to be monetized, targeting key intellectual property or preparing a destructive attack. Often the bad guys have infiltrated long before anyone realizes they've even accessed the systems. For the organization, activities to the left of the boom can include security planning and implementing tools for detection.

Everything to the "right of boom" is about responding and dealing with the fact that a security breach is now known. In the past, most organizations focused their attention on the left of boom, not the right, yet both sides of the timeline are important.

Figure 1
The timeline of a hypothetical security breach



Source: IBM Security

Figure 2
Integrating business and internal security processes is essential for crisis response

Source: IBM Security

Making better decisions during the boom event

During a boom event, an organization has the opportunity to respond well, fumble or completely lose control of its response. When a security breach or cyberattack happens, executives need to drive effective response. They must quickly instill confidence to their customers and other stakeholders that they're doing everything possible to solve the problem. For many people in the C-suite, this type of fast, intuitive response doesn't come naturally. Although they might know what to do technically to manage a breach, they often aren't prepared to cope with the human side of the equation. In a crisis situation, the C-suite is up against a human adversary, which typically isn't something that they're used to handling. Phones ringing with angry customer complaints or questions from reporters can catch them off-guard, often causing them to fall apart or do nothing. During a crisis, taking no action can be worse than taking some action, even if it's not the right action in the long run.

When a security breach or cyberattack happens, the one thing you don't have is time. Executives and members of the security team need to be able to filter the available information and put it in context, so they can quickly make the best decision. Borrowing a principle originally developed by military strategists, organizations often must "observe, orient, decide and act." Looping through this sequence encourages iteration. The idea is that if you can go through the loop more quickly than whatever you're up against, you gain an advantage. By conducting a series of responses that can be applied rapidly, you can harmonize efforts so responses aren't passive. No decision has to be final, and making small mistakes is considered better than taking no action at all.

Acting to the right of boom

The period to the right of boom involves not only mitigating the damage from an attack, but also managing the court of public opinion after customers and the media find out what happened. What happens to the right of boom can dictate the future of a company. During the crisis, executives need to display seasoned leadership, so it doesn't look like the organization is trying to hide something.

The ability to make decisions quickly is critical during and after a cyberattack or security breach. Through our research, we have found that the top cybersecurity challenge today and in the near future is to reduce average response and resolution times.[3] To handle an incident quickly, organizations don't just need procedures, they also need to practice their responses, so they become automatic.

Key lessons and recommendations

Following extensive experience running hundreds of simulations with a range of clients globally, we have synthesized three key lessons.

1. *Lead with the outcome.* A good security culture is crucial. It needs to protect the brand, reputation and future of the company. Part of that culture is, during an incident, having a clear "commander's intent" that is broadly communicated and understood. What does success look like in a security crisis?
2. *Move past paper into reality.* It's not enough to have detailed security plans and run books. What might look great on paper, tends to crumble when pressure is applied. Without regularly using and honing skills, muscle memory weakens. The entire organization needs to consistently practice, refine and test training.
3. *Leverage different backgrounds.* People with backgrounds in emergency medicine and the military usually do much better in security simulations than their colleagues with more traditional business or technology backgrounds. Because these people are used to constantly practicing, planning and preparing for many different situations, they are used to making quick decisions under pressure.

Why simulation works

If you have a heart attack, you don't want the person giving you CPR to be someone who has only read how to do the procedure in a book. In a life-or-death situation, you want the person giving your chest compressions to be someone who has practiced CPR on a dummy and developed muscle memory. That person who has practiced and rehearsed could save your life because he or she performed CPR before, even if it wasn't on a live human being.

In much the same way, executives need to understand more than crisis-response theory. They need to practice their responses so they know what to anticipate during actual security events. There's no substitute for real-life, hands-on experience, and simulation lets you practice what to do in a given situation. With a simulation, you can experience the unexpected in a controlled environment and see how you respond, and then try it again to improve your response. Imagine if you could experience a cyber breach simulation much like a pilot goes into a flight simulator to learn how to best handle emergencies.

The key to simulating a security event is to make it as realistic as possible, so people learn to work together. With a simulation, everyone from the security team, to communications and PR professionals, to the CEO can find out what it's truly like to experience a cyber attack. This type of immersive security experience can be used to test and improve employee skills, security processes and leadership across the organization. In addition to helping people cope with the event itself and the repercussions to the right of boom, going through a simulation can help executives and leaders develop better strategic long-term actions based on real events and experiences.

Improving responses

When a crisis arises, there's no substitute for planning and rehearsal. Once people have experienced a simulated cyberattack, they gain the confidence to exercise leadership and quick-thinking when the real thing happens. The best responses focus first on protecting the safety of employees and customers, then data and, finally, the company's brand. It's not a matter of *if* a crisis will occur, but *when,* so take a moment to consider these issues as you move forward:

- When it comes to incident response, is our organization practicing what we planned? Do we have a feedback cycle to incorporate the lessons we've learned?
- Do we have the right skills? What muscles do we need to exercise more?
- Does my executive team know the critical actions and decisions they need to make immediately after an intrusion is discovered?

Experts on this topic

Caleb Barlow

Vice President, IBM Security, XForce Threat Intelligence
cbarlow@us.ibm.com
https://www.linkedin.com/in/calebbarlow

Christopher Crummey

Executive Director X-Force Command Cyber Range
chris_crummey@us.ibm.com
https://www.linkedin.com/in/chriscrummey

About ExpertInsights@IBV reports

ExpertInsights@IBV represents the opinions of thought leaders on newsworthy business and related technology topics. They are based upon conversations with leading subject matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

New Orchard Road
Armonk, NY 10504
Produced in the United States of America
January 2018

26012626USEN-01

Notes and sources

1 Ponemon Institute. "2016 Cost of Data Breach Study: Global Analysis." Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC. 2016. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

2 Ponemon Institute and IBM. "The 2016 Cyber Resilient Organization." 2016. http://info.resilientsystems.com/ponemon-institute-study-the-2016-cyber-resilient-organization

3 "Cybersecurity in the cognitive era: Priming your digital immune system", IBM Institute for Business Value, November 2016