chiefexecutive.net

The CEO's Role In Preventing A Cyber Crisis

Thomas J. Parenty and Jack J. Domet

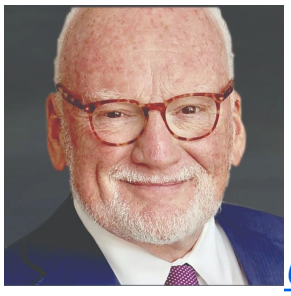
13–16 minutes

If you’re like many CEOs we meet, you assume cyber risks are best left to the experts and you have these experts in your IT and cybersecurity departments.

But the reality is that no amount of delegation will shield you from the personal consequences of a cyberattack. Following a breach, parties whose information is stolen, or whose lives are otherwise impacted, look for someone to blame. And they don’t look to your technical experts or security vendors. Upset politicians and incited media don’t blame a faulty firewall.

They look at you, the CEO. And they don’t care

who you put in charge of cybersecurity.



CYBER BEYOND SECURITY: ARE YOU READY? **Chief Executive Group's 2020 Cyber Risk Forum will prepare you to ask the right questions and keep your company ahead of fast-moving developments.** ***Keynote: Richard Clarke, Fmr. Nat. Coordinator for Security, Infrastructure Protection and Counterterrorism.*** *Learn more.*

February 24th, 2020 | The Fairmont | San Francisco, CA.

In a cyberattack, your company is technically the victim, but don't expect mercy. During a cyber crisis leadership discussion with a large critical infrastructure company in Asia, one executive told us how quickly public opinion would turn against his company if they were victimized in a cyberattack. He also noted how many parties, including politicians and reporters, can enhance

their own reputations by criticizing a company and its CEO after an attack.

With 2019 on track to rack up more data breaches in the US than the total number of listed companies on the NYSE and Nasdaq combined, the ever-increasing size and scale of cyber-attacks continue to capture both media interest and public imagination. As a result, breaches are often widely reported with over 11,000 stories about cyberattacks in US newspapers in 2019 alone.

Many people, before they even finish reading the headline of a news article about a cyber-attack, rush to blame the company and its CEO, not the hackers. The company inherits all the pent-up blame directed at poorly prepared companies that were hacked in the past.

Is this right? Blaming a company victimized in a cybercrime might seem akin to blaming a well-dressed man for being robbed, but there's a significant distinction. In the case of the robbery victim, he is the only one harmed. In the case of cyberattacks, many others are negatively affected through no fault of their own. And, again, they will almost always blame you.

Here's the bottom line: Cybersecurity is a CEO issue that can't be avoided. Just as you must personally sign off on financial statements blessed by your finance team, you'll need to approve your company's cyber defenses.

Not doing so puts you at risk. But don't worry. You can do this.

The Good News For CEOs

For many CEOs, cyberattacks can seem like business earthquakes: random, mysterious and devastating. But our research produces a silver lining for you and your executive team. Your

experience as CEO gives you most of the tools you need to effectively steel your company from a cyberattack. We've found:

• **You already have the skills you need.** CEO leadership in a cyber crisis doesn't have to be as intimidating as generally thought. Don't let the technical nature of a cyber incident stymie you. You can gain significant assurance of a company's preparedness by asking selected, nontechnical questions.

• **Preparation trumps prediction.** While foretelling the timing of a cyberattack is difficult, knowing how to prepare for a cyber crisis is not. When looking at which cyberattacks to prep for, you should give the highest priority to those that threaten your company's most important business activities and would result in the gravest consequences. Since cyberattacks can damage business activities and your company so severely, you need to consider them differently than disruptions from other causes. Water delivery is a good example of a business activity selected on the basis of significance and

impact. Loss of drinking water, especially for a prolonged period of time, can cause significant harm to entire communities, and a cyberattack can have much more widespread impact than other causes, such as physical attacks on individual pumping stations.

• **Cyberattacks don't have to catch CEOs off guard.** The types of information you need and the decisions you will face can be anticipated and deliberated long before a crisis occurs. The technical response to a cyberattack requires a properly trained team, response procedures and practice. Given prior identification of relevant cyberattacks, your company already knows where to focus this preparation.

The key is to first think about your company's most significant business risks and how a cyberattack could cause them to materialize.

Be A Cyber-Aware CEO

There's nothing like a cyber breach, and the

headlines that follow, to grab your attention. When there's a breach, all eyes will be on you to show you're aware of the seriousness of the problem. You need to swiftly show you're taking the right steps to put a ring around the damage. Showing your awareness of a cyber breach boils down to four steps:

1. Gain a rapid understanding of how the breach worked. There will always be specific details about a cyberattack that a company can't predict ahead of time. But prior consideration of cyber risks to business activities provides a starting point, with descriptions of the types of cyberattacks that could cause a crisis and the range of resulting consequences.

2. Grasp what cyber defenses were in place and why they failed. To understand the reasons why your company failed to repel a cyberattack, first look at the relevant plans for cyber risk remediation. These plans explain the cyber risk controls your company chose to mitigate the cyberattack. Further, status on the progress of the

plans gives information on where the company was on the path to acceptable residual cyber risk at the time of the attack.

3. Measure the financial and reputational hits to the company. Different types of cyberattacks result in different types of damage. Executives should consider a few common themes when deciding a course of action, regardless of the specific cyberattack involved. One is the legal implications, including your company's regulatory obligations in potentially numerous jurisdictions. In addition, setting compensation precedents could impose future obligations on your company, should similar types of damage occur later. Finally, assess damage to equipment and corruption or loss of business-critical information, and the cost of their restoration.

4. Understand what's being done to stem the attack. Once you show your awareness of a cyber breach, it's time to pivot to demonstrating you are moving quickly to contain the damage. Although avoiding and preventing cyber crises are top

priorities, prevention only works until it doesn't. If, despite all best efforts, a cyberattack succeeds, your company must be ready with a response that both counters the cyberattack and addresses the needs and expectations of affected stakeholders, all while bringing your company fully back in business. Because of your company's previous efforts in understanding cyber threats and developing cyber risk reduction plans, your company can make significant preparations long before a crisis hits. Now's the time to show how your planning is paying off.

Orchestrate A Cyber Response

A CEO demonstrating awareness of cyber threats is a great start. But your success as a CEO navigating a cyber security breach is measured by the way you react under pressure. Stepping up while headlines are flying, concerned customers are calling and politicians posturing is how you'll make a cyber breach just another obstacle you've learned to overcome. Again, in our work helping

CEOs successfully react to cyber threats, we've found winning cyber crisis leadership includes three elements:

1. Don't add insult to injury. When you're reacting and restoring your cyber defenses, it's important you don't cause any further harm or inconvenience to your customers. After a data breach has been made public, companies commonly send emails to all potentially affected individuals with instructions on what they must do to find out if their own information was included in the breach. Another common practice is to offer additional services, such as credit monitoring, but this also requires affected individuals to take action to benefit from this service. Imposing these additional burdens on affected stakeholders has two consequences, one of which is their negative reaction directed toward the company. The other consequence relates to the effectiveness of assistance a company provides. If getting the recommended help following an attack is too burdensome, individuals won't do it. That means

they will remain vulnerable to the risks your breach exposed them to.

2. Use your company's risks to build the team. Typically, the core incident response team includes cybersecurity and IT staff. Though some common skills apply to any cyber incident, the specialized skills your company's incident response team needs depend on the types of cyberattack it will likely face. For example, response to a cyberattack that uses a virus could benefit from a specialist in reverse malware engineering. An expert in computer forensics, on the other hand, will be more useful in responding to a cyber incident arising from employee financial fraud. The cyberattacks and attack techniques identified earlier help your company's cybersecurity head decide which skill sets the team needs. Depending on the nature of the cyberattack, representatives from other departments, such as legal, HR, physical security, or law enforcement liaison, augment the core team. In the case of rare or seldom needed skills, it is often practical to retain a third-party provider.

3. Say the right things to the right people. The information provided to you, as well as your decisions on restoration and accountability, provide the content for engaging stakeholders, which your company's corporate communications and public affairs departments can use as they would in any other crisis. The stakeholder engagement questions in a cyber crisis are the same as in any other type of crisis, even though the answers may be different because a cyberattack caused the crisis. Beyond addressing these stakeholder issues, your company should consider two additional questions. Will public disclosure of certain information cause harm? For example, if your company is currently under an active cyberattack, announcing it publicly could tip off the attackers and prompt them to adopt different techniques that could go undetected. In this case, disclosure undermines your company's ability to respond to an attack. Will lack of disclosure cause harm? If your company doesn't announce a cyberattack it knows about, will it expose customers and other stakeholders to new risks

they can’t mitigate because they are unaware of them?

Practice Makes Perfect

Just as you rehearse your comments for presentations, a dry run of preparing for and reacting to cyber threats will boost your confidence. Preparing for a cyber incident is one thing, but quite another to calmly it put into action. What may seem clear and straightforward written in a procedure can be challenging to undertake under fire.

But where to start? Given the number and variety of cyberattacks that could target a company, it’s impossible to prepare for all the cyber crises that could arise. We recommend CEOs consider three criteria when deciding which types of cyber crisis scenarios to practice:

1. Business impact. Practice cyber crisis leadership for scenarios where cyberattacks can cause the greatest disruption to your company’s

most important business activities.

2. Current defensive posture. Focus on crises arising from cyberattacks that are not yet fully mitigated.

3. Variety. Include a variety of scenarios affecting different parts of your company.

Cyber-Savvy CEOs: You've Got This

Yes, cyber threats are an increasing business risk you must address. But as CEO, you've navigated new risks before, ranging from accounting and counter-party financial risk to climate change and the threat from changing consumer tastes.

Successful cybersecurity leadership comes down to your own mindset. You can't take a fatalistic view that it's only a matter of when, not if, you're attacked and therefore neglect proactive protection. It's much easier if you think of a cyber crisis as a business crisis that materializes as a result of cyberattacks. That means you can rely on the crisis management systems and processes

already in place. They can also utilize the materials already prepared to manage the associated business crises. Armed with so much process support, executives can zero in on the major elements of crisis management that are affected by cyber crises.

Success hinges on upping your awareness, knowing how to respond to a breach and continuously practicing your approach. Incomplete information, uncertainty and surprises are found in every crisis. But, with some thought ahead of time, you will have the know-how and procedures to handle your company’s cyber risks. The types of technical skills and resources you will need and the decisions you will face are largely predictable and can be prepared for well ahead of a cyber crisis.