Blogs
October 05, 2020
2020: The Year COVID-19, Corporate Reputation & Cybersecurity Collided

The Fundamentals of Preparing for and Responding to a Cyber Event Are More Important Than Ever

To say 2020 has been a year of change would be quite an understatement. The COVID-19 pandemic has fundamentally transformed how we live, work, and interact with one another. This is most definitely true for the world of cybersecurity. Bill Conner, the chairman and CEO of SonicWall, probably captured it best: "We're in the midst of one of the most turbulent times in cybersecurity history. Over the past six months … we've seen shifts we thought would take decades happen virtually overnight." The abrupt transition to remote working in the early months of the year required IT departments around the world to adapt quickly—and with little precedent—in order to accommodate what could be the greatest distribution of employees and business processes in the United States. Unfortunately, the newfound challenges posed by the response to the pandemic have only intensified the activity of cybercriminals. In a June 16 hearing before the Subcommittee on National Security, International Development, and Monetary Policy, Representative and Subcommittee Chair Emanuel Cleaver (D-MO) highlighted a "75% spike in daily cybercrimes reported by the FBI since the start of the pandemic." But it is not just remote working that is causing an increase in cybercrimes. It's also the exploitation of our desire for news about current events such as the election, pandemic, and more. In short, cybercriminals are using social engineering tactics to target individuals and businesses that are working to educate themselves and stay informed. SonicWall has compared and tracked the change in the cyberattack landscape for years, and their Mid-Year Update of their 2020 Cyber Threat Report in June didn't contain much good news. Ransomware attacks increased 20% globally in the first half of the year as local governments, public administration agencies, education systems, and even hospitals were more frequently targeted due to their "softer" security. Malware, on the other hand, dropped 33%, but the attacks were more targeted and aggressive than before. Finally, attacks against the Internet of Things (IoT) devices increased by 50%, as cybercriminals directed attacks at remote employees in an effort to gain access to their work networks. With these external strains, organizations must understand the importance of handling and preparing for a cybersecurity event and the effects these events have on stakeholder trust, corporate reputation, and the bottom line. As Stéphane Nappo, the global head of information security for Société Générale International Banking, has correctly stated, "It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it." The concepts of reputation and trust are paramount for any organization as they secure their systems and data, and as they prepare for or respond to a cybersecurity event. In a December 2019 Morning Consult survey, two cybersecurity factors ranked in the top three priorities for U.S. respondents when they are considering whether to trust a company. The most important factor of respondents (73%) was how companies "protect my personal data," while the third most important factor (70%) focused on whether or not they "make products that are safe." When you read these surveys, you can't help but think about the latest retailer or business vendor you conducted business with that was hacked, the smart home devices you have throughout your house, or the various apps used for social media or to conduct financial transactions with a retailer, your stock portfolio, or for regular banking. What leaders need to understand is that trust also ties to customer loyalty. According to a June 2019 Salesforce survey, "State of the Connected Customer," 84% of customers are more loyal to companies that have strong security controls. But when those companies are hit by a cybersecurity event, that loyalty disintegrates quickly. According to the 2019 RSA Data Privacy & Security Survey, 64% of Americans report that they would blame the company—not the hacker—for loss of personal data. While trust and loyalty are important, what really gets the attention of leaders and their boards are the monetary costs. Those are very real and leave a substantial dent in the bottom line. The Ponemon Institute/IBM 2020 Cost of Data Breach Study that came out in July 2020 showed that the United States continued to have the highest data breach costs in the world at $8.64 million on average, while the average total

cost of lost business was $1.52 million. So, during these turbulent times, when the expansion of employees connecting to the corporate network from home has skyrocketed and the bad guys are working hard to take advantage of these historic shifts, what steps can companies take to address the reputational and financial burdens ahead of time? **Lesson 1: Move the Issue Deeper into the Boardroom** Cybersecurity must be a recurring topic on the agenda for board meetings. Do board members really understand the cyber risks? Are they conducting the necessary audits? Do they understand their risk appetite? Are they focused on outcomes or just processes? As Daniel Dobrygowski and Derek Vadala point out in their Sept. 2020 *Harvard Business Review* piece, "What the board really needs: a risk-oriented, holistic, and validated view of the company that considers the financial and business impacts of cybersecurity (or cyber insecurity) in a given company. Moreover, technical reports adequately capture attributes such as governance, culture, decision-making practices, or wider treatment of a company's cyber risk profile and appetite." **Lesson 2: Utilize the "When"—Not "If"—Approach** Unfortunately, as cybersecurity incidents continue to increase in occurrence and severity, many organizations continue to treat cybersecurity events as "if," not "when," events. Too often, companies have not done the simple things that will help them better respond and save money. They don't take a key maxim to heart: credibility is determined by the response to the incident, not by the incident itself. If companies would take the time to prepare for an incident ahead of time, their responses would be significantly strengthened, and they could generate savings. The Ponemon Institute/IBM 2020 Cost of Data Breach Study showed that (1) having a defined incident response team and 2) testing their organization's response in cyber simulations prior to the event saves an average of $2 million in response costs. Not only do they save money, but these simulations give leaders and their teams the opportunities to identify gaps, solve problems before they happen in real life, and get more comfortable with the subject matter. Unfortunately, too often the leaders and organizations I work with aren't as knowledgeable as they should be on this critical issue. **Lesson 3: Make Key Decisions Ahead of Time** Benjamin Franklin's famous maxim, "An ounce of prevention is worth a pound of cure," is more important than ever today. If companies haven't done the necessary preparation, they burn time the team doesn't have in the heat of the moment just getting everyone up to speed. To truly get ahead, the leadership teams should focus on getting some simple tasks out of the way ahead of time:

1. Determine your outside counsel, forensics firm, communications' counsel, and credit monitoring service ahead of time. You want to avoid adding new consultants, strategy, or leaders during a crisis, whenever you can avoid it.
2. Develop relationships with lawmakers and regulators in the states you do business. Meeting them for the first time after a data security incident is not the best way to make a first impression.
3. Segment your B2B stakeholders. Do you have customers in heavily regulated industries that might have more detailed requests from you? Are there long-time customers, partners, etc. that also need personal outreach?
4. Determine a potential escalation path for the incoming questions and requests you'll receive. How will you leverage your frontline employees (e.g., account managers, etc.) the heads of lines of business and your general counsel and CISO, and who will you hold in reserve for white glove customers, policymakers/regulators, or other critical stakeholders.

Lesson 4: Manage the Message Communicating the right messages at the proper points in the lifecycle of a cyber event will have a significant impact on how a breach is reported. While developing messages should not be one-size-fits-all, the following are key principles to live by:

1. Focus initial messages on the steps being taken to investigate the issue and frame it as a criminal issue.
2. You have integrity until you don't. Companies need to realize cybersecurity incidents always include twists. What you think you know invariably turns out later to be inaccurate and, if communicated, may cause significant legal liability issues. While rumors and misinformation will swirl, companies must understand investigating a data breach and communicating about it properly and accurately takes time. "In major breaches, it can take a month or two of round-the-clock work to answer: How did the attackers get

in and when? What did they view? What did they steal? Are they still in there?" explained Eric Friedberg, co-president of Stroz Friedberg, LLC and Aon's Cyber Solutions Group. If you must communicate something, say what you know, acknowledge what you don't know, and continue to keep people updated.
3. Think through what you put out on your social channels, what you stop posting, and also how to respond to your stakeholders in social media.
4. Set up the appropriate customer/media/social monitoring and listening posts to see how the information about the incident is being received, so you can make adjustments to the communications in real time.
5. Live out your corporate values as you treat your customers as your North Star.
6. However, don't neglect the wide variety of stakeholders interested in breaches including policymakers, regulators (state and federal) and industry stakeholders (e.g., payment brands).

Lesson No. 5: Learn the Language Finally, in a cybersecurity event, it quickly becomes evident when many of the players don't understand the technical issues or the language of cybersecurity. A chasm is immediately created between the IT team and the other parts of the business. That's why it's vital for the full response team to know the nomenclature of the IT security and payments worlds. Spending some time with a free online resource, such as the National Initiative for Cybersecurity Careers and Studies, will pay off when disaster strikes. While taking these steps won't take all of the sting out of the cyber event, it will significantly lessen the pain once the issue has surfaced and allow the company to focus on the problem at hand. *David J. Chamberlin is a managing director at CRA, Inc., where he partners with leaders to strategically drive business results, build trust and credibility, strengthen relationships with stakeholders, and successfully navigate and mitigate the critical issues affecting their organizations. He previously served as the CCO at PNC and the CMO at SonicWall.*

Explore more in

Privacy & Security