The CEO's Cybersecurity Responsibility in the Corona Virus Chaos

By Dr. Keri Pearlson and George Wrenn
MIT Sloan School of Management
March 27, 2020

COVID-19 has impacted our organizations in many ways including creating new cybersecurity threats. As C-level executives, we are concerned about the health and safety of our teams and colleagues and about the financial impact of the sudden shift of customers and financial markets. But we need to add security to our growing list of concerns as bad actors are already finding new and nefarious ways to exploit the chaos to their advantage. CEOs have a personal role to play today in securing the company today.

Hackers Take Advantage of The Chaos

Hackers are creative and, much like improv actors, adjust tactics and behavior to fit the current events. COVID-19 has provided the perfect storm for hackers as fear, uncertainty and doubt permeate through our organizations. For example:

- According to the annual Verizon cybersecurity study, executives have over a 10 times likelihood of being targeted in email phishing attacks, and the current crisis has caused an increase is attempts.
- Recent Check Point Research found a spike in coronavirus domain name registrations, exceeding 50,000 new website domains. Some of these sites are actually set up by hackers to exploit those seeking information about the virus (and those sites seek money or plant malware on devices who access them).
- Experian has reported a sharp rise in identity theft attempts via SMS/Text message scams.
- Law enforcement has seen an increase in COVID-19 related scams, including "fake medicine" to treat the illness.
- A new phenomenon named "Zoom Bombing", presumably a nod to the previous idea of "Photo Bombing" where unintended people or graphics are introduced into a picture or video stream, has swept the Zoom user base to the point where Zoom created a warning page on their blog in an attempt to help users block these attacks.

Put this all together and you have a perfect storm for attackers bent on exploiting your company during a time of global crisis. With most organizations opting for remote work, the attack surface for would be attackers has increased exponentially including interrupting conference calls and phishing attacks using COVID-19 fears as bait to take over employee devices and access our networks. Our well-known business environments have turned chaotic in a matter of days where the urgency to respond can cause quick, and sometimes well-intentioned but ill-conceived responses. All of which may lead to business loss or fines, landing squarely on the CEO's desk.

How do we make sure our organizations are cybersecure in this time of COVID-19?

The increase in vulnerabilities and attacks also suggests something unique: an opportunity for CEOs. Cybersecurity in the time of COVID-19 is not a fiduciary responsibility or leadership challenge for the technology team. This is a time for executive leadership to step-up activity and communications to build strong believes, attitudes and values for everyone on the team about their personal role to help heighten vigilance against opportunistic cybersecurity threats to the organization.

Our research at MIT's Sloan School of Management suggests that successfully changing the values, attitudes and beliefs of employees is done in part through the behaviors and communications of senior leaders. When senior leaders make cybersecurity a priority and firmly instill it in messages to employees, it sends a very strong signal to the team, and makes it a priority for employees too. Our research on building a culture of cybersecurity suggests that

CEOs must act now to drive cybersecure behaviors of employees during this time of crisis and beyond. Here are three things executives can do today:

1. **Executives must make cybersecurity a personal priority and "walk the talk".** Simple actions like making sure to not click on emails or open links without checking if they are real are cybersecurity hygiene everyone needs to follow. Using extra security measures such as dual-authentication and passwords to protect online meetings are more important than ever today. The CEO must personally do everything he/she can to both keep his/her digital world safe, and to role-model it for others.

2. **Executives must set up a culture of cybersecurity for the whole organization**. Senior leaders must let everyone know that they are making cybersecurity a personal priority. Simple actions like short weekly email reminders from the desk of the CEO about things like not clicking on emails that might have phishing links, or sending out details on how to prevent intruders in their remote meetings, sends a very different message than an email from the technical leaders. It clearly shows that this is important to the CEO and that is should now be important to every employee.

3. **Executives must give extra support to your digital colleagues.** Meet with security and technology teams. Listen to their immediate concerns and needs and provide a way to increase support. Perhaps create cross-functional "task forces" to address these issues immediately so the business impact is minimized. For example, new email filters, teleconference access methods or other lines of defense may be needed. This is a time to make sure technology supports business needs while increasing security, and that requires increased discussions between executive leadership and technology leaders.

Conclusion: Criminals know that a great time to attack is when there is high levels of fear, uncertainty and doubt. COVID-19 has created this perfect storm. Now is the time for the C-suite to step in and instill the values and attitudes that every employee has a role in keeping the company secure. This is not another training class. This is a time for executive leadership to demonstrate their personal commitment to keeping the company secure by personally upping their activity, telling team members that they are doing so, and supporting those who are your first responders in times of cyber-crisis. We believe that kind of leadership will go a long way instill the same priority in every employee. And that might just save our companies from new vulnerabilities that have arising in this time of chaos and COVID-19.

Dr. Keri Pearlson is the Executive Director of the research group Cybersecurity at MIT Sloan (CAMS). She is also an entrepreneur, consultant, author, and teacher with numerous publications and case studies on topics at the intersection of strategy, organization design, and information systems. She received her Doctorate from the Harvard Business School and holds a Master's and Bachelor's from Stanford University.

George L. Wrenn is a graduate fellow and researcher at the MIT Sloan School of Management. He is also the Founder of LetoSecurity. He holds a Bachelor's degree from Harvard University, has been a graduate fellow for over a decade at MIT and has completed executive programs at Oxford University Saïd School of Business, Harvard Business School and the University of Cambridge.