THE ENTERPRISERS PROJECT

A community helping CIOs and IT leaders solve problems

Search Search

Supported by Red Hat

ArticlesCIO ResearchWhat is an Enterpriser?About This Project

3 ways leaders can build a stronger security culture

3 ways leaders can build a stronger security culture

COVID-19 gives bad actors new opportunities: Now's the time for executive leadership to step up and focus everyone in the organization on security

14 readers like this

By Keri Pearlson | George L. Wrenn | June 29, 2020

In this time of COVID-19, C-level executives are concerned about the health and safety of their colleagues and about the financial impact of the sudden shift of customers and financial markets. Now we need to add security to the growing list of concerns, as bad actors are already finding new and nefarious ways to exploit the chaos to their advantage.

Leaders have a critical and personal role to play in securing their company.

Hackers take advantage of the chaos

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

- Recent Check Point Research found a spike in coronavirus domain name registrations, exceeding 90,000 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 that 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.
- Zoom bombing 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.

[Want to avoid Zoom bombing and other surprises? read Zoom tips: 6 ways to make meetings better.]

Put this all together and you have a perfect environment 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 to take over employees' devices and access our networks. 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 to build a culture of cybersecurity: 3 tips

The increase in vulnerabilities and attacks also offers a unique opportunity for senior business leaders. Cybersecurity in the time of COVID-19 is not a fiduciary responsibility or challenge for the technology team alone. This is a time for executive leadership to step up activity and communications to build a strong culture of cybersecurity that guides everyone on desired actions and behaviors. Executives, particularly CEOs, can personally help heighten vigilance against opportunistic cybersecurity threats to the organization.

Our research at MIT's Sloan School of Management suggests that successfully changing the culture, or 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.

CEOs and other senior business leaders must act now to drive secure behaviors by employees during this time of crisis and beyond. Here are three things executives can do today to build and reinforce a culture of cybersecurity in their organizations:

1. 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 examples of cybersecurity hygiene everyone needs to follow. Use extra security measures such as dual authentication and passwords to protect online meetings and add an additional layer of defense against malicious hackers. Executives must personally do everything they can to keep their digital world safe and to model best practices for others.

2. Bring cybersecurity into the light

It's important for leaders to make cybersecurity a personal priority, but it's also important to talk about it often with the organization. To establish a culture of cybersecurity for the whole organization, senior leaders must let everyone know that they are making cybersecurity a personal priority.

Here are some simple actions we have seen work, according to our research:

- Send out a weekly email reminder from the desk of the CEO sharing ideas and examples of desired behaviors, like not clicking on emails that might have phishing links.
- Share personal examples the leader has seen or read about, such as recent hacks or new vulnerabilities (such as fake websites for personal protective equipment whose link loads malware onto company computers, or phishing emails that purport to assist COVID-19 patients with new medications).
- Ask your team at the beginning of your next meeting for stories or examples they have seen.

These kinds of behaviors send a very different message than an email from the technical leaders about how important cybersecurity is to the company.

Everyone expects the CIO and CISO to talk about keeping data secure. Hearing it directly from other C-level executives changes the culture of the organization. It clearly shows that this is important to the CEO and that it should be important to every employee.

3. Give extra support to your digital colleagues

Meet with security and technology teams regularly to learn and participate in business impact discussions. 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.

Make culture change a long-term goal

Criminals know that a great time to attack is during periods with high levels of fear, uncertainty, doubt, and chaos. Now is the time for the C-suite to step in and instill the values and attitude that every employee has a role in keeping the company secure.

MORE ON SECURITY

- 4 ways to always be improving security
- How to secure the home office: 8 priorities
- Remote work: 6 common misunderstandings about online security threats

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 what they are doing, and supporting your first responders in times of cyber-crisis. We believe that kind of leadership will help instill the same priority in every employee.

We all hope the COVID-19 pandemic is a temporary situation, but keeping our companies secure is a long-term goal. Building a culture of cybersecurity where everyone feels a personal responsibility to assist in keeping the company secure will help protect our companies from new vulnerabilities for years to come.

Dr. Keri Pearlson will moderate the panel "Keeping our organizations cyber-secure in the COVID-19 environment. How secure are we?" for the MIT Sloan CIO Digital Learning Series on July 15th. Register here.

[How can automation free up more staff time for innovation? Get the free eBook: Managing IT with Automation.]

SUBSCRIBE TO OUR NEWSLETTER

Stay on top of the latest thoughts, strategies and insights from enterprising peers.

Enter your email address...

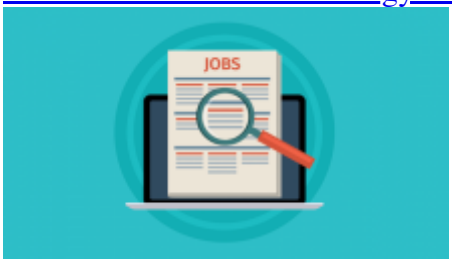
Select your country or region

SUBSCRIBE

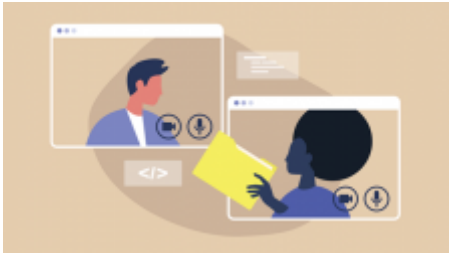
Privacy Statement

Related content

[IT talent 2020: How technology leaders are adjusting strategies]



[IT careers: How to write a resume in 2020]



[Security jobs: What's hot and what's cooling]

Tags:

- IT Strategy
- Security

No comments yet, Add yours below

Comment Now

Your name *

E-mail *

The content of this field is kept private and will not be shown publicly.

Homepage

Comment *

Notify me when new comments are posted

Accept the Terms of Use to continue. You are licensing your contribution(s) as CC-BY-SA. *

I'm not a robot
reCAPTCHA
Privacy - Terms

Submit Comment

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.
» More about me

George L. Wrenn is a graduate fellow and researcher at the MIT Sloan School of Management. He is also the Founder of LetoSecurity.
» More about me

Dr. Keman Huang is a Research Scientist at Cybersecurity at MIT Sloan. His research focuses on cybersecurity operations and management. Prior to his role at MIT, he was a faculty member at Tianjin University He holds a Ph.D., and two bachelor degrees from Tsinghua University.
» More about me