Guidehouse

guidehouse.com

EXECUTIVE INTERVIEW SERIES

Cyber Resiliency During and After the COVID-19 Pandemic

Q&A with Guidehouse Cybersecurity Leader Marianne Bailey, a Former NSA and Pentagon Executive

April 2020

Tell us about your experiences as deputy national manager for U.S. national security systems at the National Security Agency (NSA).

In this role at NSA, I was responsible for ensuring that the U.S. national security systems — those systems that the U.S. deems critical to protecting national security — were sufficiently protected against cyberthreats. This not only includes all our Department of Defense (DoD), intelligence community, and government networks that process classified information, but also our planes, ships, tanks, satellites, radios, launch vehicles/ranges, all communication devices, and more.

I also had responsibility to produce and certify the nation's cryptography that protects these systems, as well as many systems of our foreign partners. It involved strong partnerships with industry and government agencies and spanned developing security standards, producing keys and codes, leading assessments and testing, providing systems security engineering support to development activities, creating awareness and training, and supporting DoD and White House policy development. It is a very important job for our country, and I was honored to serve in that position.

Given the COVID-19 pandemic, what are the major steps organizations need to take to ensure their organizations are cyber-resilient?

First and foremost, organizations should send a reminder to their entire workforce about cybersecurity best practices.

As we've already seen, cybercriminals do not hesitate to take advantage of crisis situations. **Interpol recently issued a "purple notice"** warning 194 countries to be on the lookout and exercise vigilance against cybercriminals. During these times, employees and customers operate outside of their norm and exceptions are often made to ensure that critical work can continue. But employees often do not step back to understand the ramifications of their actions; for example, clicking on one malicious link, which may at first seem very valid, could bring an entire organization to a halt. To make those emails and links more appealing, cyber-criminals target what appears to be relevant and extremely interesting information regarding the latest COVID-19 information.

There are some basics to help employees remember what actions they need to perform. First, remind them to access company information from a company-approved device and to connect to the company network through an approved virtual private network. They should also confirm that their devices' patching is up to date.

Next, make sure they understand social engineering and how this makes threats like "spear phishing" possible. The more information that is available about you publicly, the easier it is for a cybercriminal to prepare an email that employees are likely to open. And, remind them to refrain from installing unapproved software on devices.

Moreover, organizations should identify their critical assets and perform due diligence to protect them. One example that has plagued organizations is that they fail to understand their connectivity to third parties. They do not recognize where their data travels and/or the data they are legally bound to protect. Therefore, they do not know how that data is protected as it leaves their boundaries. I've been involved in many assessments where we have identified 10 times the number of connections to third parties and industry partners than companies had self-identified.

The COVID-19 pandemic also reinforces the need for organizations to reassess their cyber-resilience, prioritization of IT operations, and dependence on data resources related to mission fulfillment. This is essential, considering constraints in available staff due to illness or reduced inefficiencies related to remote working and access.

> **“First, I highly recommend that every organization develop an incident-response plan before they have to deal with a breach.”**

To ensure a secure cyberposture, organizations should review and address high-priority vulnerabilities by:

- Removing legacy software from operations. If a vendor is no longer patching the software, you should not be using it.
- Listing approved apps and denying unapproved ones.
- Implementing strong identity and access management.
- Applying patches in a timely fashion.
- Tracking technology assets so they remain in control of owners and users.
- Utilizing modern security technology to monitor network and device anomalies.

This is the perfect time for an organization to review its cybersecurity posture, and they should consider getting an independent assessment of how they are doing.

For organizations that have experienced a breach, what are best practices to respond and mitigate the situation?

First, I highly recommend that every organization develop an incident-response plan before they have to deal with a breach. Determining what steps to go through, who you need to have involved, and how to respond technically to the incident in a crisis situation is never a good idea.

Guidehouse runs incident-response tabletop exercises to help organizations prepare for a breach before one actually occurs. We also have an offering that helps organizations prevent a breach.

Both the SANS Institute and the National Institute of Standards and Technology have excellent guidance outlining the steps in the technical mitigation process.

Often, organizations that experience a breach will respond to and mitigate that specific breach. Upon recovering from the breach, they should perform an assessment of their cybersecurity posture and consider other areas where the company may be weak, the risk associated with these weaknesses, and what can be done to mitigate them. Otherwise, they will likely find themselves dealing with another breach soon.

Cyberbreach Response Best Practices

- Identify individuals who need to be involved in responding to the breach, to include business leadership, legal, board members, forensics, cybersecurity, data privacy officers, CIO/IT, communications/PR, and/or investors.
- Identify roles and responsibilities for each of these groups related to the breach response.
- Conduct a forensics investigation to identify the specifics of the breach, develop remediation steps, and retain evidence.
- Stop the data loss.
- Develop a communications plan.
- Determine who must be notified.
- Develop a notification plan.

What are main misconceptions organizations have around cybersecurity?

There is an old cybersecurity saying: The weakest link is all that really matters. Cybercriminals look for the area that is the easiest to penetrate in an environment. They study their targets and understand companies' partners, the technology they use, and the employee practices.

For starters, many leaders don't believe they will have an adversarial cyber event, or if they do experience one it will not be significant.

Some organizations still believe cybersecurity is the responsibility of the IT department, but the reality is it is everyone's responsibility.

Furthermore, it can be very difficult to explain at an executive level the business risks associated with a cyber incident. But phishing attacks are often directed at executive leadership because that tends to be the most lucrative place and the easiest target.

It is all about translating very technical information into corporate risk, and this risk can affect many areas. It can be financial, due to legal ramifications; for example, a breach can result in both civil and criminal lawsuits for not meeting legal requirements in protecting data. It can be a reputational risk as clients and customers will lose faith that the company is a safe place to do business. It can be a huge financial burden as companies may not be able to perform their business for a significant amount of time as they recover from malware or ransomware.

And, of course, there is the direct cost of technical recovery and response to the actual breach, which might involve rebuilding parts or all of your IT environment.

What do you see as the biggest cybersecurity threats and opportunities in the next year? The next 3-5 years?

The rapid growth of technology is both a significant threat and opportunity. Innovative technology and the expansion of 5G capabilities is going to bring millions of user devices to the world. Whether it's medical implants, smart cities, or autonomous vehicles, these devices will ensure real-time information is available to those who need it to manage their lives and businesses.

In addition, the remote way we are operating today as a result of COVID-19 will set the stage for our future business environment. Companies are learning quickly that they can operate very effectively and efficiently while employees work remotely. But the increase in the sheer number of users communicating virtually creates more data and more connections than ever before. All of this data becomes more accessible, and that can be good and bad.

A cybercriminal will look for weaknesses in the technology, its implementation, or the user operation to do damage. The implications are only limited by the innovative applications for this technology. For example, malware can have major impacts on an autonomous vehicle, robotics on an automated factory floor, on a medical device administering medicine or restarting your heart, or on an energy grid providing electric distribution to customers. It is critical that as we embark on this new innovative way of life, we demand security is designed-in at inception and implemented and monitored during operations.

In the past few years we have experienced cybercriminals and nation-state actors responding to U.S. policies with unconventional cyberattacks beyond government systems. As the U.S. and our foreign partners continue to adopt more technically sophisticated, automated, and interconnected capabilities, we should expect these attacks to grow in numbers and impact. Building in cybersecurity at inception that is interoperable with today's and tomorrow's automated monitoring and response systems is the only effective way to defend against these cyberthreats.

Marianne Bailey
Cybersecurity Leader
M (443) 535-1698
E **mbailey@guidehouse.com**

linkedin.com/company/guidehouse-health

twitter.com/guidehouseHC

guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology, and risk consulting. We help clients address their toughest challenges with a focus on markets and clients facing transformational change, technology-driven innovation and significant regulatory pressure. Across a range of advisory, consulting, outsourcing, and technology/analytics services, we help clients create scalable, innovative solutions that prepare them for future growth and success. Headquartered in Washington DC, the company has more than 7,000 professionals in more than 50 locations. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit: www.guidehouse.com.

Guidehouse