Know Your Network

How the New Normal in Business Is Reshaping Cybersecurity

BROUGHT TO YOU BY COMCAST BUSINESS

The dramatic rise in cyber threats and shift to remote work have businesses tapping new tools and expertise.

Before Covid, one in 30 companies had half of employees working remotely. That share is expected to jump 900%, with one in three companies supporting remote work at that level, according to a study by Mercer. As organizations adjust to such a big transition in such a short period of time, they're particularly focused on cybersecurity.

The distributed workforce — where some employees are in the office and some are remote — presents a host of new cybersecurity challenges. With employees working from home, often connecting via their home networks and in some cases using their personal devices, it can be far more difficult to authenticate legitimate users. The security industry has also seen a major uptick—spikes as high as 500%—in phishing, social engineering, and DDoS attacks from bad actors seeking to capitalize on the health crisis.

We talked to cybersecurity consultant **Tyler Cohen Wood**, former executive director of Cyber Risk and Workforce Development for CyberVista, and **Shena Seneca Tharnish**, VP of Cybersecurity Products at Comcast Business, about how enterprises should be rethinking their approach to cybersecurity.

How have the cyberattacks that companies face evolved since the start of the pandemic?

Tyler Cohen Wood: Social engineering attacks are usually based on fear and urgency, and with Covid, people are afraid. Hackers know this, and they use it to their advantage. We have seen many sophisticated phishing attacks that claim to offer Covid help, but they are well-crafted attacks.

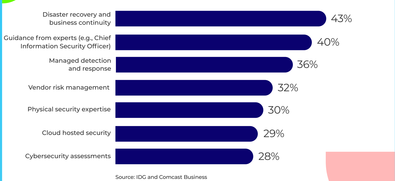
Shena Seneca Tharnish: Approaches like phishing, malware and denial-of-service attacks are being used to exploit businesses, and we're seeing much higher rates of attempted attacks. These are targeted threats using tried-and-true tactics that have been around for many years, but now the network topology has shifted and traditional defense plays are less effective. One of the best long-term solutions to cybersecurity in its current state is to try to segregate your business connectivity from the residential connectivity as much as possible.

IDG and Comcast Business

Shifting Cybersecurity to Support the Expanded Remote Workforce

Read the Report →

Where Organizations Need Help With Cybersecurity



Source: IDG and Comcast Business

What are the cybersecurity solutions that enterprises have used in the past that may fall short in this new environment?

SST: Single sign-on without multifactor authentication won't work anymore when companies have most of their workforce coming onto their network from the outside, maybe with a VPN connection. You're trusting that what's on the other end of that network connection is, in fact, your employee. Adding a layer of multifactor authentication lets you validate that the user is, in fact, trusted.

TCW: Companies may want to re-evaluate bring-your-own device policies that have worked in the past to make sure that those policies are up-to-date and fit in with a company's overall risk management strategy. Everyone should have a company laptop, and, ideally, a work phone, as well, especially for those with access to sensitive data. The work phone should not have anything personal on it, no social media, no web browsing—it's only for work.

What network cybersecurity solutions are essential for the transition to a remote-first workforce?

SST: Capacity was an immediate need that the companies had to address to support a remote workforce. Companies put in more bandwidth capacity for internet connectivity, as well as more infrastructure and license capacity for higher simultaneous workloads for things like session counts and VPN.

VPN provides connectivity back to internal business systems. And with so many applications in the cloud, web security to block malicious phishing, malware and botnet sites, is essential.

As dependency on internet connectivity becomes more crucial to operations, bad actors are disrupting businesses with distributed denial of service attacks. While next generation firewalls can defend against lower volume attacks, service provider DDoS mitigation can help defend against volumetric attacks and avoid loss of service.

+400%

Phishing email attempts more than quadrupled in March 2020.

Source: Bloomberg

In a recent IDG survey, 99% of IT decision makers said that they will need managed security services as they expand remote work capacity. How can managed security services help companies meet these cybersecurity challenges?

SST: In today's environment, the need for greater security is essential. Companies are considering managed services for several reasons. First, they get another set of eyes on their network in a time of resource constraints. Another reason is that skilled cybersecurity talent is scarce.

An enterprise can benefit from managed security service providers because these providers can monitor the company's network for threats and detect risks and issues. And then they can respond with remediation in a more timely manner than the company itself may be able to, which frees them up to focus on their core business.

+300%

DDoS attacks more than tripled in the second quarter of 2020.

Source: Kaspersky

Many of the business changes we're seeing today will likely remain in place for the long term. How can companies take a long-term approach to cybersecurity as well?

SST: It's important to have multiple layers of defense. If you can't isolate your employees, you should ensure that remote access and endpoint protection are current and configured optimally on all devices, as well as set up for frequent automatic updates.

TCW: Companies of all sizes are aware of the importance of having a robust cybersecurity approach that is sustainable and scalable over time. We'll see companies adopt a more collaborative approach, with technology and employees working together to combat cyber threats. AI will play a bigger role in threat detection and mitigation, adapting to existing and new threats and learning how to better protect enterprise networks and systems.

Protecting data is paramount, of course, but what are some other reasons that organizations are so focused on cybersecurity right now?

SST: Having strong cyber resilience can be a competitive advantage, especially when it's at the forefront of their operations and their commitment to their customers, because users are much more attuned to the impact of cyber threats today than they used to be. Customers will gravitate toward businesses that offer cyber assurances or some level of protection versus those that don't. You don't have to be a cybersecurity company, you just have to care about it and express that you're following best practices. Having good security not only helps protect your business from threats and breaches, which could be costly due to outages and remediation, but security could also boost your brand reputation.

TCW: The biggest advantage is risk avoidance. Companies that are agile adapt to cyber threats faster and are better positioned to deal with threats as they happen. Companies that are typically slower to adopt cybersecurity solutions fall behind and are at greater risk.

Know Your Network

Know Your Network explores how tech decision makers can use network technology to enhance their business

The Future of Work

Can Technology Turn Remote Work into a Competitive Advantage?

Read Now →

Business Agility

The Technology You Need for the Work-Anywhere Future

Read Now →

Business Agility

The CIO's New Mandate: Deliver Digital Agility Now

Read Now →

Customer Experience

Network Solutions Create Digital Agility for Businesses

Read Now →

Customer Experience

Expert Advice on How to Enhance CX With Software-Defined Networks

Read Now →