Cyberattacks Put Every Enterprise at Risk

Techniques diversify as corporate adversaries get smarter

By Paul McLane

EDITOR'S NOTE: Welcome to Future's third edition of Need to Know, a series exploring complex topics and how they apply to each industry served by our websites and magazines.

"We keep building new things on old infrastructure that never seems to get fixed."

Chris Wysopal is a hacker who was quoted in a column in *The Washington Post* about the state of internet security (or perhaps we should call it "insecurity"). In May, Wysopal — also known by his hacker name, Weld Pond — joined several others in a return visit to Capitol Hill, where 20 years prior they had testified in a congressional hearing about the insecurities of software and networks.

Their 1998 appearance helped put the issue of cybersecurity on the national stage. A central part of their 2018 message is that digital security isn't much better today.

Need to Know More?

Have a burning question about cybersecurity, or maybe a request for a different topic you'd like to see us tackle? Email us at needtoknow@nbmedia.com and we'll put our top minds on it!

Costly and Dangerous

Malicious cyberactivity cost the U.S. economy between $57 billion and $109 billion in 2016, according to the White House Council of Economic Advisers. Cyberthreats are ever-evolving, and the sophistication of adversaries keeps growing. But the private sector may, for any number of reasons, be tempted to underinvest in cybersecurity, according to the White House report.

National security officials echo the concern.

"Our daily life, economic vitality, and national security depend on a stable, safe and resilient cyberspace," the U.S. Department of Homeland Security said in explaining why it devotes a large web resource to the topic.

The department this spring released a strategy hoping to help reduce vulnerabilities, build resilience, counter malicious actors, and make the ecosystem more secure. It identifies 16 "critical infrastructure" sectors where a loss of networks would have a debilitating effect on the country. But even trying to define those sectors demonstrates how broadly the subject touches every corner of American life; they range from commercial facilities and manufacturing to the communications sector and health care.

DHS took particular note of a growing concern about the threat of "wide-scale or high-consequence events" that could cause harm or disrupt services on which the economy and millions of people depend. "Sophisticated cyberactors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy or threaten the delivery of essential services," the report said.

How might your own business be whacked? A threat can come via denial-of-service attacks; destruction of data and property; disruption of business, perhaps for ransom; and the theft of your proprietary and financial and strategic information. Reports of data breaches and cyberattacks are everyday news. Lewis Morgan of the IT Governance Blog curated more than 60 such stories in the month of May and counted the total of breached records that month at more than 17 million — "actually quite low when compared with previous months."

In 2018, virtually every major and minor business or organization relies on the global, interdependent IT ecosystem. The degree to which leaders take the subject seriously could, in the long term, determine the survival of those enterprises.

To learn which trends businesses should be watching, we turned to several sources approaching the topic from various angles.

Threats in Bursts

In its *2018 Annual Cybersecurity Report*, Cisco said malware is definitely becoming more vicious and harder to combat. "We now face everything from network-based ransomware worms to devastating wiper malware," the report said. "At the same time, adversaries are getting more adept at creating malware that can evade traditional sandboxing."

While encryption can enhance security and is used by roughly half of global web traffic, Cisco continued, encryption provides bad actors with a powerful tool to hide command-and-control activity. "Those actors then have more time to inflict damage."

Artificial intelligence may help. "Encryption also reduces visibili-

IOT POSES NEW CYBERSECURITY THREATS FOR CABLE

BY GARY ARLEN

AS CYBERCRIMES and incidents of institutional hacking increase, cybersecurity is a critical concern for big TV distributors that give consumers access to the internet.

It's also a strange topic for cable operators, though, because it's rarely discussed in public, beyond the chorus of concern from consumer data watchdogs.

The FCC, whose leaders have made lofty speeches about the importance of cybersecurity, offers a perfunctory summary of its cybersecurity objectives, with few details about its cable or telco initiatives, in describing the agency's Cybersecurity and Communications Reliability (CCR) Division.

NCTA-The Internet & Television Association and the American Cable Association emphasize that "the entire cable industry takes cybersecurity very seriously." Both groups back security and risk management practices, but details about those efforts – or the failures in the system – are scant.

Still, the scale of cyberthreats to the cable industry is significant and growing. In Akamai's Summer 2018 State of the Internet/Security: Web Attack report, the firm measured a 16% increase in the number of distributed denial of service (DDoS) attacks recorded since last year globally, with new and more devious attack methods noted.

Steve Goeringer of CableLabs

There are also constant reminders of new threats. This past May, researchers found that U.S. customers' WiFi connections could be harvested from a cable operator's bill or email. Comcast said it quickly disabled the vulnerability in its activation portal, established an additional layer of authentication and that no personal user info was ever accessed.

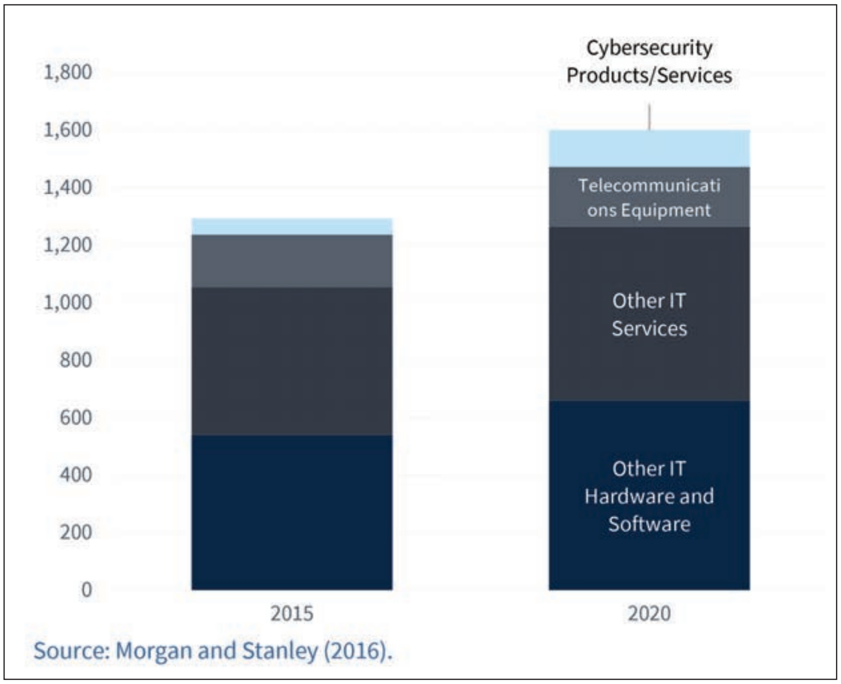
Cable has been "at the forefront of cybersecurity of broadband" thanks to the DOCSIS cable-modem specification, which has employed strong encryption and authentication since its version 1.1, CableLabs principal security analyst architect Steve Goeringer said. Subsequent updates have created further barriers to DoS and DDoS, he added.

"Delivering services the way they were intended, including protecting customer privacy, is always critical," Goeringer said. He cited pirated over-the-top content, which aside from being illegal, also exposes consumers to malicious software and theft of personal information, and the growing presence of Internet of Things devices, which are often insufficiently protected and can bring malicious software into the system.

Kyrio, a CableLabs subsidiary that provides technology services, has been focusing on Internet of Things security. "Companies that can provide strong security at scale will be able to use that as a key differentiator for their products, protect their brand and future-proof their products," Ron Ih, the company's director of business development, said in a June 4 blog post. Putting an emphasis on cable's growing involvement with wireless services, he observed that, "expanded wired and wireless connectivity accelerates the need for a more scalable security solution for these networked devices" in the IoT value chain.

CableLabs vice president of technology policy Rob Alderfer recently acknowledged the need for government/industry cooperation, especially in the fast-emerging IoT category.

"With the constant barrage of new cyber incidents, often driven by IoT devices vulnerable to exploitation, governments at all levels are taking notice and grappling with the rapidly evolving threat," according to a CableLabs summary of his remarks at an IoT workshop. "Cybersecurity is no longer the domain of the IT department, but rather a key area of governance for all enterprises."



Source: Morgan and Stanley (2016).

Projected investment in cybersecurity (in billions of dollars).

ty," Cisco added. "More enterprises are therefore turning to machine learning and artificial intelligence. With these capabilities, they can spot unusual patterns in large volumes of encrypted web traffic. Security teams can then investigate further."

Cisco noted several other trends and findings:

- Short, pernicious "burst attacks" are growing in complexity, frequency and duration. "In one study, 42% of the organizations experienced this type of DDoS [distributed denial of service] attack in 2017. In most cases, the recurring bursts lasted only a few minutes."
- Many new domains are tied to spam campaigns. "Most of the malicious domains we analyzed, about 60%, were associated with spam campaigns," Cisco reported.
- Security is seen as a key benefit of hosting networks in the cloud. "The use of on-premises and public cloud infrastructure is growing. Security is the most common benefit of hosting networks in the cloud, the security personnel respondents say."
- One bad insider can be a big threat, and a few rogue users can have a huge impact. "Just 0.5% of users were flagged for suspicious downloads. On average, those suspicious users were each responsible for 5,200 document downloads."
- It's not just your IT assets that are at risk. Expect more attacks on operational technology (OT) as well as the Internet of Things (IoT). "Thirty-one percent of security professionals said their organizations have already experienced cyberattacks on OT infrastructure."
- The multivendor environment affects risk. "Nearly half of the security risk that organizations face stems from having multiple security vendors and products."

Another observer taking stock is Aidan Simister, global senior VP at Lepide Software, an IT auditing, security and compliance vendor.

Writing in a post on the *CSO* website, Simister predicted artificial intelligence will take a bigger role. Though AI may help the good guys, he noted, hackers can use it to launch more sophisticated cyberattacks.

IoT Ransomware

Further, new strains of malware can work around "sandbox" defensive techniques, waiting until they are outside the sandbox before executing their malicious code. Meanwhile, Simister agreed that the Internet of Things could become more of a target for ransomware, with hackers targeting power grids, factory lines, smart cars or home appliances to demand payment.

Many businesses, Simister predicted, will not comply with the European Union's new General Data Protection Regulation on data protection and privacy (the thing you've been getting all those emails about). He predicted some companies would choose to ignore it, accepting the risk.

A growing number of companies are also likely to adopt multifactor authentication in response to data breaches involving weak, stolen or default passwords.

Simister said he expects that more sophisticated security strategies may find wider adoption. These could include the use of "remote browsers"; deception technologies that imitate a company's critical assets; systems to spot and identify suspicious behavior; better network traffic analysis; and "real-time change auditing solutions" that do things like detect abuses of user privileges or suspicious activity in files and folders.

Simister, though, also sees the risk of more attacks backed by hostile governments; in response, he predicts more efforts to train staff and to develop international sharing of information.

"Nearly half of the security risk that organizations face stems from having multiple security vendors and products."

– Cisco Systems, *2018 Annual Cybersecurity Report*

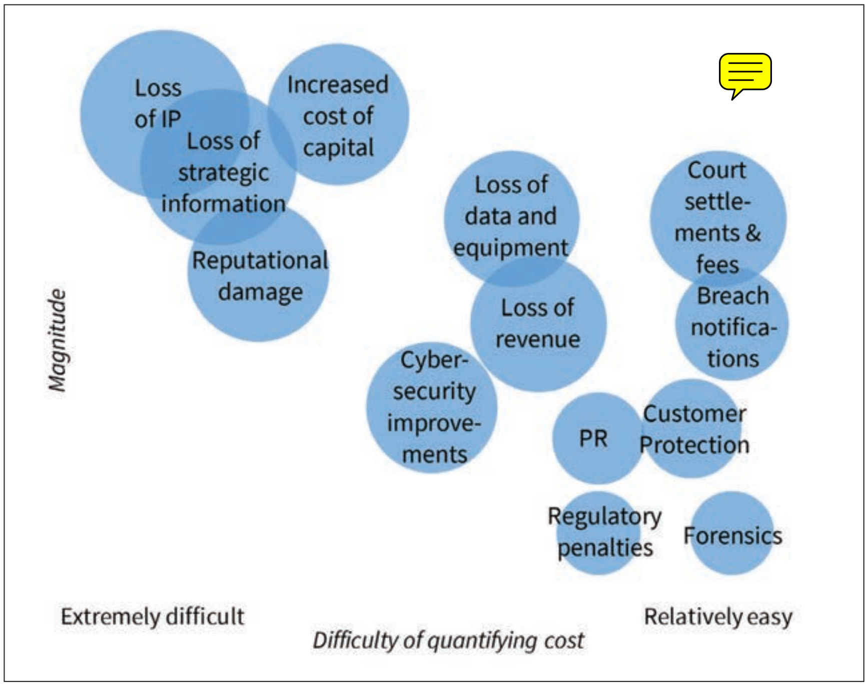
One change in mindset visible in the market is a de-emphasis on the idea of "perimeter security."

Privacy Paradox

"You are not safe behind the perimeter, because the perimeter itself no longer exists," Akamai argued on its website. "Today's world is cloud- and mobile-driven, and the traditional moat-and-castle approach to enterprise security is no longer applicable for modern business practices."

With applications hosted in various places and a workforce on the move, the company said, there is no longer a delineation between inside and outside the network. "As a result, seemingly every week there are new reports about high-profile data breaches and cyberattacks."

Akamai chief technology officer Charlie Gero has argued in favor of what he calls zero-trust security architecture. "Companies must evolve to a 'never trust, always verify' zero-trust model to secure against the wide variety of threats that exist and are constantly evolving," Akamai stated.



An "adverse cyberevent" can cost your business in numerous ways. This graphic is from a report by the White House Council of Economic Advisers.

Looking at the consumer economy more broadly, cybersecurity is only likely to become more crucial thanks to ongoing developments in areas as diverse as cryptocurrency, interactive smart speakers and mobile payments.

For example, a major trend toward platform personalization — whether it be on Facebook, Spotify, Wave or NextDoor — raises the privacy stakes. Venture capitalist Mary Meeker of Kleiner Perkins Caufield Byers noted the massive amount of personalized data that people have put into such platforms.

That data improves engagement and leads to better experiences for consumers, but it also helps creates what she calls a privacy paradox, she said in remarks at the Code 2018 conference: "Internet companies are making low-price services better in part from user data. Internet users are increasing their time on internet services based on perceived value. Regulators want to ensure data is not used improperly, and not all regulators think about this in the same way."

Regulatory considerations are thus a big, uncertain element in this picture.

The Weak Human Link

Security should be an ongoing process, but it often tends to be treated as a one-time, set-it-up-and-forget-it event, said Wayne Pecena, assistant director of information technology for educational broadcast services at Texas A&M University and director of engineering for KAMU Public Radio and Television. Rather, cybersecurity is a never-ending concern.

"It is a continuous process of monitoring, evaluation, analysis and prevention as the threat landscape is always in a state of change and evolution," Pecena said.

"I would also not lose sight of the past, as ransomware, phishing [and] distributed denial of service will likely continue at an accelerated pace," he added. "As cloud services and applications continue to expand, I would also keep the cloud cybercrime landscape or Cybersecurity-as-a-Service (CaaS) on my radar."

In Pecena's experience, most organizations do spend plenty of time and money in protecting their IT environment, but often the simplest areas can be overlooked while the focus is on higher-tech matters.

"Social engineering remains one of the largest threats to an organization, and the human factor remains a weak link," he said. "The Internet of Things movement brings challenges, as most of these types of devices lack any real internal security capability and instead rely on external protection means."

He also finds "crypto-mining" to be a fascinating area of concern as computing resources are hijacked for someone's bitcoin mining applications. "Not necessarily destructive — like DDoS or ransomware — to an organization, [but] host computing resources can be [affected] such that legitimate application use is impacted. Malicious mining scripts can easily be picked up from a casual website visit, and this opens a new area for antivirus protection software."

For Pecena, this recalls the days of desktop computers being unknowingly hijacked to serve music or distribute porn.

Those well-meaning hackers who returned to Washington recently hoped to draw attention once again to the issue of digital security. At least one pushed for government to play a larger role. But another said companies also need to take advantage of the tools and knowledge that are already available.

It was Robert Mueller — yes, that one — who is credited with saying back in 2012 that there are only two types of companies: those that have been hacked and those that will be hacked.

Today that wisdom is often updated to read: "There are two types of companies: Those that know they've been hacked, and those that don't know they've been hacked."

Manage accordingly.

Paul McLane is managing director, content, of Radio World *and the Future TV/Radio/Video group.*

MORE ONLINE
For article sources and additional information, go to broadcastingcable.com/July2.