FORESCOUT®

2020

Cyber Predictions

2020 Cybersecurity Predictions

It's that time of year again, where we sit down as a team and discuss what trends we expect will accelerate, and new ones that will emerge over the next 12 months. What struck us this year as we narrowed down more than 50 predictions to our final eight was just how quickly the cybersecurity industry is changing. Threats and attackers are becoming more sophisticated and continue to wreak havoc upon businesses—regardless of size or industry—with no signs of deceleration.

That means companies need to be more strategic when it comes to advancing their security controls. It also means they must get a handle on effective, up-and-coming security technologies—many of which we talk about on this list—before they become mainstream. That includes adopting new technologies, as well as protecting the latest devices. It also means considering some of the implications a cybersecurity attack could have on some of our most foundational assets, such as critical infrastructure.

While we can't put every significant trend on our list, we have chosen ones we think will be particularly impactful in 2020—trends that are bold, timely and likely to impact our customers. Take a look.

FORESCOUT

2020 Cyber Predictions

1 Artificial Intelligence (AI) Takes Off in the Industrial Sector

Industrial companies will continue to shift toward AI solutions for analysis of cybersecurity data. This is part of a broader trend of companies adopting tools that can efficiently and effectively automate tasks, such as workforce challenges, cost/benefit analyses and everyday security needs. More and more companies in this sector will use AI and machine learning tools to leverage data and augment human decision-making.

Industrial companies are looking for ways to better protect their critical infrastructure devices, the vulnerabilities of which have become more apparent in the past years given the growing number and increasing severity of attacks on power utilities and manufacturing plants. CISOs are looking for tools that can help them with this problem, and AI has the potential to flag anomalous activity that could point to an attack and analyze sensor data for more effective responses to security threats and even address predictive maintenance needs. This is important because downtime in critical infrastructure environments can be catastrophic. AI is far from a silver bullet, requires extensive expertise and is still largely in early technical innings, but demand for it will grow in 2020 and beyond.

2 5G Gets Very Popular

The market for 5G infrastructure technology is expected to reach $4.2 billion and two-thirds of companies intend to deploy 5G in 2020, according to Gartner. 5G technologies allow businesses to replace existing networks with a lower-latency, higher-bandwidth alternative, letting them connect more types of devices and gain enhanced capabilities around technologies like AI, edge computing and automation. This presents a significant opportunity for companies to advance their technology posture.

As 5G adoption spreads, so do potential security threats associated with these technologies. Companies will reach a critical mass of these devices in 2020, forcing them to reevaluate their risk paradigm for connected devices. Further complicating that paradigm is the fact that devices leveraging 5G could potentially bypass some traditional cybersecurity technologies by connecting directly to cellular networks. It's unclear if this changing risk paradigm will result in an attack or breach in 2020 due to the newness of the technology, but regardless, companies will have to consider changing their security strategies or leave a growing group of devices without adequate protection.

3 No Surprise: More Regulations

The U.S. federal government will continue to evolve mechanisms for evaluating the cyber postures of departments, agencies and government contractors. As part of this effort, the Federal Information Technology Acquisition Reform Act will be replaced by the Agency-Wide Adaptive Risk Enumeration
algorithm, and the Cybersecurity Maturity Model Certification will supplant NIST 800-171.

The federal government will also continue to mature its capabilities to provide guidance and assistance to key sectors, especially the power sector, through programs from the Department of Energy/Office of Cybersecurity, Energy Security, and Emergency Response and Department of Homeland Security. Through these efforts, it will put pressure on the power and healthcare sectors to improve, with calls for more robust regulation of health delivery organizations and calls for North American Electric Reliability Corporation Critical Infrastructure Protection to be reimagined.

4 The Rise of Disruptionware

In 2020, disruptionware will increasingly intersect with connected systems and rogue devices in building automation and operational technology (OT) systems. These disruptionware attacks include ransomware, but also reach more broadly to include disk-wiping malware and similarly disruptive malicious code. In recent research, Forescout noted the rise of disruptionware across industries, particularly manufacturing, as it relies heavily on OT technology. These attacks can be incredibly impactful on a business. For example, companies affected by LockerGoga in 2019—including U.S. chemical companies Hexion and Momentive—were forced to replace entire systems infected with the malware. Other companies hit by the NotPetya ransomware, including Spanish food distributor Mondelez and Danish shipping firm Maersk, estimated their losses to be $100 million and $300 million from the attacks, respectively.

We expect to see many more of these attacks in 2020. We also believe there will be at least one big attack on a major energy or manufacturing company that will severely disrupt the company's operations. This event will serve as yet another wake-up call to CISOs to reconsider the IT/OT convergence inside their own companies, evaluate technologies like network segmentation, which will allow them to protect these systems. It will incentivize federal and state regulators, who will put more pressure on power, manufacturing and healthcare sectors through more robust regulation.

5 CISO Roles and Responsibilities Expand

CISOs have increasingly assumed responsibility for securing OT networks as those networks converge with IT networks. In fact, IT and OT networks have increasingly overlapped, with 84% of organizations already adopting or planning to adopt an IT-OT convergence strategy in 2019, according to SANS. To date, that trend of IT-OT convergence has largely been a technical one. However, it's a trend that will expand in 2020 to become a cultural one. As CISOs increasingly assume responsibility for securing OT networks, many more companies will choose to combine the IT and OT security teams into one cohesive organization. This will require not only a cultural shift as the teams come together, but also new skills and training for IT, OT and hybrid IT-OT teams. It will also necessitate the creation of roadmaps for how IT and OT will work more closely.

Some CISOs may also choose to further combine the security teams with the network or other teams inside of the organization in an effort to create even more efficiencies. A few organizations have already started doing this, with the idea that security will be more integrated throughout the enterprise.

6 Healthcare Security Gets Better

Hospitals will finally start to shift how they procure Internet of Things (IoT) medical devices in 2020. This will happen in recognition of the attacks these organizations have seen in the past few years. While security will not always outweigh other factors, such as cost, licensing, support, or type of device, it will increasingly become a high-priority consideration in the buying and procurement process. This becomes increasingly important as the number of IoT devices in healthcare rises by an anticipated 2 to 3x in both IT and OT.

In many companies, there will be bigger budgets and more commonplace projects to secure devices that are either prohibitively expensive or impossible to update or replace. Overall, in both cases, healthcare organizations will move up the maturity model for cybersecurity in 2020. However, those that do not follow this trend, particularly small- and medium-size organizations, will continue to face devastating cybersecurity threats.

7 Windows 7 Support Expires

Windows 7 transitions to “end of life” on January 14th, meaning Microsoft will no longer support or regularly update the system with fixes when a security vulnerability is found. Like what we saw with the end of life of Windows XP, history will repeat itself in 2020, with at least one major attack that takes advantage of a resulting vulnerability. WannaCry is one example of the kind of devastating effects an unpatched, out-of-date operating system can have. The attack leveraged the EternalBlue Windows vulnerability as an entry point, then spread laterally across organizations. Microsoft had issued a patch for this vulnerability, but organizations that hadn’t applied it or those running out-of-date operating systems, such as Windows XP, were still vulnerable.

There are multiple reasons organizations could choose not to upgrade, even if the operating system poses a security risk. For example, the device may be running critical software that won’t work appropriately on a more recent version of Windows, like Windows 10. But those who choose not to upgrade or do not take other appropriate mitigating measures such as network segmentation will put themselves at increasing risk over time.

8 Cloud Migration Causes New Security Headaches

Financial services companies have been accelerating their adoption of cloud technologies as part of digital transformation strategies. But this migration from the data center to the cloud can increase cybersecurity challenges, driven by factors such as misconfigurations of networking devices and business application servers that lead to exposure of critical data. This is particularly concerning as more financial services companies migrate more of their critical business applications and workloads to the cloud.

We predict that this acceleration in cloud migration will result in a massive data breach in 2020, the size of which could be as significant as the Equifax fiasco, given the amount of data these companies hold and their increased willingness to migrate critical data and applications to the cloud.

Conclusion

What these trends all have in common is that they will require companies to be more strategic when it comes to advancing their security controls in 2020. Companies in every industry will need to get ahead of emerging and growing technologies—like 5G, AI and the cloud—and consider how their existing technologies may pose new threats in today's cybersecurity landscape. To do that, they should reflect on how their existing tools fit these trends and others that might affect them in 2020 and, if needed, adapt strategically and consider new technologies that can help protect against an attack or limit its impact.

The good news is that, while all signs point to attackers growing stronger and more sophisticated, the cybersecurity industry is also becoming more robust. Innovation is at an all-time high and customers are the benefactors of that. Together, we can strategically tackle this challenge and emerge from 2020 stronger than ever.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com