CYBER SECURITY CONCERNS FOR THE NEW DECADE

AMD COMMUNICATIONS

55 Main Street, Suite 315,
Newmarket, NH 03857
(888) 704-3183

www.amdcomm.com

The last 10 years in cyber security resemble little so much as a war. One side advances, the other side repulses that advance and shores up its defenses. Then the first side advances somewhere wholly different. This constant back-and-forth has left us all in a delicate position. Not only are the cyber security forces of a business forced to respond to actual attacks staged against networks, but they're also left to guess where the hackers and similar bad actors will strike next. Worse, they must work to formulate a defense against attacks no one has ever seen before.

With that in mind, let's take a look at the recent history of cyber security and consider how best to employ cyber security resources going forward.

THE HISTORY OF CYBER SECURITY...SO FAR

While cyber security has been a major issue since "cyber" anything existed, the rapid growth of online and mobile activities from 2010 to 2019 brought with it a host of new issues.

The "Nation-as-Hacker."

The 2010s brought with it the first incident of an entire country serving as the basis for a hack. Google revealed Operation Aurora, which was a substantial hit on its Chinese infrastructure. The resulting hacks hit over 50 separate companies on the internet and were ultimately found to be an effort to identify Chinese intelligence operatives in the United States. The notion that a nation could use its resources—commonly much larger than any corporation could muster—to hack a business meant attacks could now be orders of magnitude larger than previously believed.

The "Nation-as-Hack-Target."

The 2010s also revealed that nations were increasingly being targeted in hacking as well. In July 2011, a defense contractor had been hacked and in the process lead to 24,000 files from the Department of Defense being stolen as well. Subsequently, this led to a 2013 meeting where the North Atlantic Treaty Organization (NATO) announced it had developed a complete

cyber-defense capability that was expected to be online later that year.

Ransomware on the rise

Starting with "the unnamed Trojan of 2011," ransomware saw a substantial spike upward in the 2010 to 2019 period. With Cryptolocker, WannaCry, and a host of others emerging, there were more types of ransomware to face down than ever. Moreover, ransomware set its sights on more targets than before. From businesses to municipalities to private users, ransomware knew no boundaries and targeted whatever it could find.

WHY BUSINESSES NEED TO ADJUST THEIR COLLECTIVE CYBER SECURITY MINDSETS

The history of cyber security – both recent and long-term – shows that businesses need to fundamentally change their cyber security mindsets. Many other concepts add their own urgency.

A whole lot of change

Just taking a look at the last 10 years in cyber security makes it clear that businesses need to change the way they think about security. We had ransomware go from an occasional nuisance to one of the biggest attack classes around. We've seen threats that didn't even exist 10 years ago show up out of the blue. The notion that the older modes of cyber security would continue to be valid in the face of a threat environment that hasn't stopped changing in a decade just doesn't hold up.

A massive demonstrated threat

It wasn't so long ago that the biggest victims of cyber security issues were regular people – people whose bank, email, and social media accounts were hacked. Now, we've seen an increasingly large number of major corporations hit by attacks. 57 million Uber drivers and riders. Just shy of 150 million Equifax customers. 3 billion Yahoo accounts. Hacking is no longer retail, it is increasingly wholesale, and there's less and less the regular person can do to prevent it. With the regular person much less a target and the major corporation now

firmly in the crosshairs, the responsible business must step up to address the matter or risk a huge loss of face in the market.

An increasingly complex attack

We've seen that the nature of the target has changed but so too has the nature of the attack used to pursue the target. This isn't surprising; the kinds of attacks that would work on Joe Sixpack down the street or the Ma and Pa Kettle Phone Company wouldn't work very well against the likes of an AT&T. The sheer difference in available resources precludes any such possibility. The attacks, therefore, must become that much more complex and powerful. Even trying to document such an attack is difficult for cyber security professionals – let alone trying to repel it – so businesses need to fundamentally reconsider their response to such attacks.

Wild changes in response mechanisms

With new kinds of attacks coming out on a regular basis, it's no surprise that the tools designed to respond to these attacks are changing as well. A recent study found that 61% of enterprises responding say they "cannot do without AI technologies when it comes to detecting breach attempts." Companies not turning to artificial intelligence (AI) in breach detection, therefore, are behind the eight ball. Respondents in that study also noted that – in 48% of cases – the budgets for AI in cyber security were going to increase. What's more, they would increase an average of 29% in 2020 alone.

WHAT TO EXPECT IN CYBER SECURITY THREATS. SO FAR. MAYBE.

While trying to predict the future in a rapidly-shifting environment with any kind of accuracy might seem like trying to sculpt fog in a windstorm, there are some trends that are increasingly likely to play a role in the next decade of cyber security threats.

Ransomware on the decline

It's not going away, but back in 2018, it started to become clear that the rates of ransomware attacks were dropping. Essentially, the warnings about ransomware seem to have taken hold, and businesses—and even regular consumers—are taking steps to make ransomware's impact much less.

Remember, the main threat of ransomware is the locking up of a single PC or potentially a network's worth. If the information on these devices is stored elsewhere— such as a cloud backup or an air-gapped backup PC—then ransomware is a minor threat.

AI will continue to gain

We've already seen this prediction asserted as fact as businesses are expected to spend more on AI protection in 2020. This actually sets the stage for future AI development as well. For those businesses that haven't yet picked up AI protection tools, it will become increasingly necessary. Since those businesses with AI are better protected, those without will likely become targets of hackers looking for a successful run. Thus, businesses will have to pick up AI tools to improve their protection. This in turn should yield excellent conditions for AI tools, which means more offerings in the field and more options.

Spending increases will also continue

This is a very small leap of logic. With more tools available – and the price of failing to defend systems only escalating – companies will spend more on their own defense. They will have more reason to spend, and more tools to spend on, making conditions ripe for continued spending growth when it comes to cyber security tools.

World Cyberwar One?

We've already seen how – in the last 10 years – the notion of nation-as-hacker and nation-as-a-hacking target both emerged. These particular genies will likely not go back in the bottle. The increase in attacks between and among nations means that the chance of a complete cyber-based war—or a war that incorporates these tactics as part of warfare—will increase. Moreover, it's become clear that nations—especially first-world industrialized nations—increasingly depend on their computerized systems, so attacking these will strike a much greater blow than any missile, bomb, or rifle ever could.

Changing threats, struggling response

Here's a combination problem that should give anyone pause. Supply chain attacks are expected to increase in some quarters, since these are ripe targets that are increasingly vulnerable thanks to the growth of Internet of Things (IoT) applications. However, an ongoing and worsening problem in finding security talent to repulse these attacks is also plain. One study found that 70% of respondents cited finding security talent as a major problem, and six months later that number increased to 91.3%. Gains like those in so short a time make it apparent that more and newer attacks will arrive, and we may not be up to facing them.

FOREWARNED REMAINS FOREARMED

While trying to prepare for every eventuality in cyber security threats and movements remains as impossible as it ever was, having a handle on the most likely problems to come will remain the best way to address future threats. Being prepared for cyber security issues often starts with expert advice, so reach out to us to address your cyber security issues now before they can become serious problems. Our blend of expert personnel and powerful tools will offer the best chance at protection against tomorrow's threats in whatever form they take. Drop us a line to get the process started.

AMD COMMUNICATIONS

55 Main Street, Suite 315, Newmarket, NH 03857
(888) 704-3183 | **www.amdcomm.com**

55 Main Street, Suite 315, Newmarket, NH 03857
(888) 704-3183
www.amdcomm.com

AMD
COMMUNICATIONS