COVID'S IMPACT ON CYBERSECURITY PLANNING

"Trust but Verify."

These three words ring as true in today's cybersecurity world, as they did when Ronald Reagan first shared them with Mikhail Gorbachev, then-Soviet Communist Party General Secretary, some three decades ago as the Cold War melted away. At the time, there was no Facebook, Amazon, or Netflix, and the Soviet people enjoyed a steady and predictable media diet of Channels One… and Two.

While COVID-19 has rendered offices and meetings passé, we as a society have moved much of our communication, purchasing, and general interaction directly to the internet. Zoom, Slack, Teams, and WeChat dominate—and people suddenly seem busier than ever. We have more to juggle today, remotely, and all of it is channeled through our home communication systems. The implications of this for the cyber industry are enormous. A new and unforeseen pandora's box has popped open, gifting yet another point of vulnerability and access for nefarious actors to exploit.

CYBERSECURITY'S LATEST PANDORA'S BOX

Employees who had worked in an office prior to COVID-19 often used a desktop computer, logging on at a specific time, and working a particular shift. Much of corporate employee activity was routine and predictable, enabling internal corporate security teams to quickly assess when activity deviated from the norm.

That was six months ago. A study by the National Bureau of Economic Research in June notes that 50% of US employees are now working remotely or from home. The new reality has shifted the 'office' to 'home-work environments'—in fast forward.

Following the move to remote working, companies gave employees laptops to use in their homes, which, in many instances, became a computer shared with kids playing Fortnite, and for other personal matters. Passwords used for website access and payment processing became the password for accessing corporate systems. Log in credentials for websites switched to 'single-login' pathways linking corporate devices to personal accounts on social media, banking properties, and e-commerce sites.

This shift easily compromises home WiFi networks. Possessing even limited information about the resident's primary user, kids, and pets' names, effectively gives criminals the code to your front door lock keypad. With mobile (non-corporate system) access spiking to 38% in March 2020 compared to March 2019[1], home computers, tablets, and smartphones are now today's tools of commerce.

Vulnerabilities are only going to rise from here. The remote work environment represents our society's new normal. In short, we should consider transforming 'Trust but verify' to 'Verify, then Trust'.

1 https://www.statista.com/statistics/1106863/covid-19-daily-in-home-data-usage-change-us-2020/

WHAT DOES TODAY'S CYBER LEADER LOOK LIKE?

Today's cyber leaders are more battle-tested than they were even six months ago—and this field testing has birthed a new generation of cyber leaders. The new generation of cyber warriors is more flexible, adaptable, and less tethered to 'standard operating 'procedures and more traditional approaches. He/she expects constant change and transition, and pro-actively seeks out adversaries often lurking in open sight and in the web underworld.

Today's cyber warrior looks a lot like Kobi Lechner, who until recently ran Wix.com's IT security infrastructure. A global, multi-lingual executive with startup experience complemented by service in more formal corporate settings, Kobi keeps his hand in the game—and finger on the trigger—by serving as Non-Executive Director and Board Advisor to several early-stage, dark web, and anti-hacking technology operations. He deploys commercial skills and battlefield knowledge to an ever-shifting cyber landscape, coordinating with a loose network of similarly minded individuals in Silicon Valley, Shanghai, and Sao Paolo.

The cyber battles of today offer no time to convene a National Security Council meeting or run Bomb Damage Assessment calculations. If you don't act and react quickly, your client, IT system, data, and reputation can be radically and irreparably compromised. And this is exactly how Kobi operates—much like the warfighter who leverages fifth-generation jets and drones integrating land, sea, and air forces in real-time for analysis, attack, and counterattack. Kobi mentors up-and-coming cyber leaders to always expect the unexpected.

This is what the life of the cyber leader of tomorrow looks like—anticipating, probing, looking for the adversary's soft underbelly, and when necessary, taking the new cybercriminal out.

"…BUT WHO IS THIS ENEMY?"

Call him what you may: enemy, adversary, hacker, cyber-Mafiosi—the simple fact is that business is good for nefarious actors today and is, only getting better.

Today's cybercriminal is amorphous, hides behind servers housed in less-regulated lands, deploys false flag operations, and on occasion, masquerades as a corporate citizen. This individual continuously benefits from technology developments and is quick to adapt to cutting edge apps.

The FBI's Internet Crime Complaint Center (IC3) registered almost as many internet-related fraud and swindle complaints as they did during the entirety of 2019, during the first five months of 2020. Companies operate in fear of attack, and when attacked, quickly capitulate, transferring funds to 'make this go away.'

And the music isn't slowing down anytime soon….in fact, this symphony is currently supported by a number of even more sophisticated and powerful instruments! Technology companies contribute to enemy capabilities by resisting calls for data sharing and device access, pushing law enforcement to leverage commercial solutions to track, chase, and very often, neutralize bad actors. The larger these technology service providers grow, the more detrimental this all becomes to the ordinary citizen.

Governments will intervene, for sure, if the companies do not destroy each other first. The recent Fortnite revolt against Apple and Google is an early harbinger of what is to come. Utilities, retail, municipal governments, online e-commerce, Industry 4.0, digital manufacturing, media, and transportation underpin our daily existence, and we rely on all these industries to mitigate—and eliminate—latency.

If these industries do not (cannot?) take offensive action to ward off bad actors, what will the Karens and Kens of the world do? Rendering any of these industries inoperable can potentially lead to a cascade of crises—the least damaging of which might actually be energy supply, communication, water, or transportation impairment.

SO, WHAT'S THE PLAN, STAN?

The pandemic has hammered home to the technology community that we should trust (employees, partners, service providers, and even employers) though we must continuously verify—and stay on the lookout for malfeasance. Translation: contingency and backup planning is more important than ever.

Cybersecurity executives' dexterity is being tested at a time when IT staff are working remotely from home offices, and systems are under siege with incessant phishing probes and creative attacks. Many of these attacks are often followed up by ransomware demands, data theft, and outright extortion.

Leaving decisions up to technology, or robots - or bots, or bits - or whatever you might want to rely on for your company's crown jewels, is a losing bet. This is no longer a game of multi-factor authentication, password verification, or 'my CISO has it all covered.' CEOs and Boards are more exposed today than ever before in history and will be on the hook for shareholder value losses, reputational compromise, and worse.

The Gipper had it right that cold December day in 1987: "Trust but Verify." He could not have predicted, however, how prescient his rhyming Russian proverb ("Doveryai no Proveryai") would indeed become.

AUTHOR

Martin Mendelsohn
Senior Partner