Cyber Talk

CYBER SECURITY IN THE NEW NORMAL
STRESSORS AND SOLUTIONS

The notion of a cyber security breach can prompt any business professional to start panicking. Against the backdrop of the coronavirus pandemic and the corresponding technological transformations, 53 percent[1] of business leaders state that cyber security and data loss represent "major concerns". This anxiety isn't new, but here's what you should know...

Although many organizations have cyber security mechanisms in-place, apprehension around cyber attacks has reached epidemic proportions. This is due to changes in the computing environment: the increased volume of employees working from home, the corresponding remote access infrastructure, a massively increased dependency on cloud apps, and more sensitive data in-motion than ever before. The balm to this scourge lies in dramatically improving security measures.

The Distributed Work Stress Test

In March of 2020, as the coronavirus pandemic emerged, hundreds of thousands of offices closed and millions of workers adjusted to the distributed work model. The dangers of the pandemic, combined with delayed government-level responses and other external factors left people frazzled and fallible. Cyber criminals quickly capitalized on the frenzy.

For weeks, uncertainty around the spread of the contagion mounted, and attackers eagerly preyed upon these fears. Amidst voluminous uncertainty, alerts about the coronavirus, personal protective equipment, and virus testing easily proved tempting for the crooks. Phishing websites popped up across the web and 2.2 times[2] more individuals fell for phishing threats than usual. One in four Americans received a phishing-related email.[3]

1 "Survey of 53 business leaders shows that cybersecurity and data loss are major concerns as the pandemic continues to drive digital trends," by Joe Mullich, BusinessInsider December 21, 2020.

2 "Scam Pandemic: How Attackers Exploit Public Fear through Phishing," by Marzich Bitaab, March 23, 2021.

3 Phishing in a Pandemic: 1 in 4 Americans Received a COVID-19 Related Phishing Email, by Open Text Coporation, Sep 22, 2020.

Email Phishing

Over 90 percent of cyber crimes begin with an innocuous-looking email.

A given criminal may attempt to impersonate a well-known organization or may make an email appear as though it originates from a common brand, such as Walmart, Costco, Amazon, Zoom, Google[4] or Microsoft.

One phishing email rocketing around the web arrived with the subject line "You have been added to a team in Microsoft Teams." What well-meaning employee wouldn't believe that, given the nature of remote work?

Microsoft reports that its O365 email platform contains features to protect against phishing. Google reports blocking more than 18 million[5] coronavirus-related emails on a daily basis. To put this in perspective, as the Ebola virus gripped West Africa from 2014-2016, researchers witnessed an increase of two-hundred thousand[6] scam emails containing falsified Ebola updates; not millions of emails.

---

4 "Coronavirus cyber-attacks update: beware of the phish," by Check Point Software, May 12, 2021.
5 "Google says it blocks 18 million COVID-19 related scam emails each day," by Nathan Eddy, HealthcareITNews, Apr 17, 2020.
6 "Scam Pandemic: How Attackers Exploit Public Fear through Phishing," by Marzich Bitaab, March 23, 2021.

THE TOP 10 MOST COMMONLY IMITATED BRANDS

Microsoft
CHASE
yahoo!
amazon
Rakuten
DHL
IKEA
LinkedIn
PayPal
Google

SMS-based Phishing

Worse yet, most employees rely on mobile devices for work purposes. Research shows that people frequently stumble across phishing schemes on mobile devices. The probability of an employee falling for an SMS-based phishing attempt that could precipitate a major business compromise is all-too-real.

Protecting employees from phishing attacks requires extensive and well-thought-out user education. It can also help to invest in an end-to-end cyber architecture that's designed to block deceptive phishing websites. Get cutting-edge anti-phishing tools that can secure all of your organization's attack surfaces.

The Cloud's Contribution to Concerns

Why else are CISOs in a heightened state of anxiety? As recent distributed workforce shifts took shape, teams quickly transitioned to or scaled their cloud architecture. In an overwhelming effort to keep teams productive in the short-term, cloud security took a backseat. Some teams lacked the IT experience to ensure correct cloud security set-ups.

Eight-four percent of cloud engineering teams that completed the workforce transition expressed concerns about security vulnerabilities embedded into the new environments. They had adopted new access policies, networks, and devices in order to optimize remote work capabilities. The fact that there was much to learn left a lot of room for error.

Misconfigurations

Historically, cloud security misconfigurations always represented a source of worry. However, as teams began to manage distributed working infrastructure, concerns surrounding misconfigurations multiplied. As many as 92 percent[7] of cloud security experts angst over the fact that their organization may be vulnerable to a misconfiguration-related breach.

In 2017, the US Pentagon made an AWS configuration error that led to the exposure of data.[8] "If something [an organization] of this size and importance suffers from the same problem, we need to start taking it a lot more seriously," stated researcher Chris Vickery.[9]

Compliance

With the initial cloud transitions complete, and misconfigurations avoided, organizations are now wondering about whether or not their configurations remain in compliance with regulatory requirements. An unclear understanding of compliance leaves a business vulnerable to fines and litigation. For organizations that contend with health data specifically, full visibility into system operations is fundamental.

Should organizations consider ditching the cloud for the data center, post-pandemic? The cloud affords organizations as much as 25 percent[10] in cost savings annually and can provide a competitive advantage. To eliminate anxiety around the cloud, organizations should simply work to manage and secure resources.

---

7 "Cloud Security Risks Rise During the Coronavirus Pandemic: Survey," by CISOMag, April 20, 2020.

8 "Pentagon exposed some of its data on Amazon server," by Selena Larson, CNN Business, Nov 17, 2017.

9 "Pentagon exposed some of its data on Amazon server," by Selena Larson, CNN Business, Nov 17, 2017.

10 "Banks' Inevitable Race To The Cloud," by Ron Shevlin, Forbes, Jul 22, 2019.

In securing the cloud within the new hyper-connected landscape, an increasing number of IT teams are embracing multi-layer cloud security. In addition, automation and machine learning are becoming a part of the new normal. Advanced cloud security not only protects your cloud. It can also help protect your networks and mobile devices.

HOW? With shared threat intelligence through a consolidated security solution, you can spot threats to multiple elements of your system in tandem.

Managing Remote Access: Critical Infrastructure Stressors

Critical infrastructure systems serve as foundational elements of industries, from transportation, to the energy sector, to telecommunications. Critical infrastructure owners and operators rely heavily on industrial control systems for day-to-day functions. Modern configurations of these systems are often vulnerable to attack. In 2020, more than 360[11] industrial control system vulnerabilities were disclosed within the first six months of the year alone. Over 75 percent of those vulnerabilities were described as "critical" or "high" risk.

Previously, the risk to industrial organizations was limited due to the complete separation of physical operations from electronic environments. For pandemic-related reasons, amongst others, many owners have upgraded systems to leverage remote access. However, the implementation of proven and effective remote access solutions "may not map perfectly to control system environments", as CISA states. As a result, much anxiety surrounds the deployment and maintenance of remote access for industrial control systems (ICS) landscapes.

11 "Industrial control system cybersecurity vulnerabilities are rising in 2020," by Brandon Vigliarolo, TechRepublic, by August 19, 2020.

2,000% + increase in attacks on ICS and SCADA architecture.

Remote Access: ICS Management and Data Loss

Due to the analog nature of maintenance, a certain level of trust used to exist between system operators and field devices. Now, the trust between the operator and the field device can evaporate in an instant.

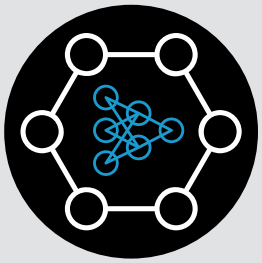
An adversary can quickly compromise control system or administrative networks. With remote access, the physical security of ICS systems is not within the purview of the system operator. The operator can no longer inherently trust the devices. This creates an unfamiliar form of distress for ICS groups.

Remote Access: Vendor Services and Security

In current control system environments, vendors commonly arrange for remote support capabilities. This enables the timely delivery of services. However, in many circumstances, vendors request access in a way that circumvents the system operator. As a result, the vendor may accidentally mishandle privileges or unintentionally ignore threats. From a cyber safety perspective, this operator/vendor configuration raises security concerns. It speaks to the need for ICS operators to work closely with vendors, and for vendors to adopt strong cyber security countermeasures in conjunction with their clients.

Remote Access: Larger Security Challenges

When considering remote access in the context of ICS, partners, supply chain vendors and MSP providers can all create cyber security threats. Given the potential magnitude and impact of an ICS attack, how can ICS owners ever sleep well at night? There are seemingly too many plausible scenarios that could result in a cyber incident.



Maintaining the integrity of industrial control systems is tough. Strategies must be multi-pronged and must pertain to policies, best practices, system owners, system operators and all others who digitally interface with an ICS. Experts recommend that organizations invest in cyber security solutions that couple network segmentation with automation and threat intelligence.

More Data In-Motion Than Ever

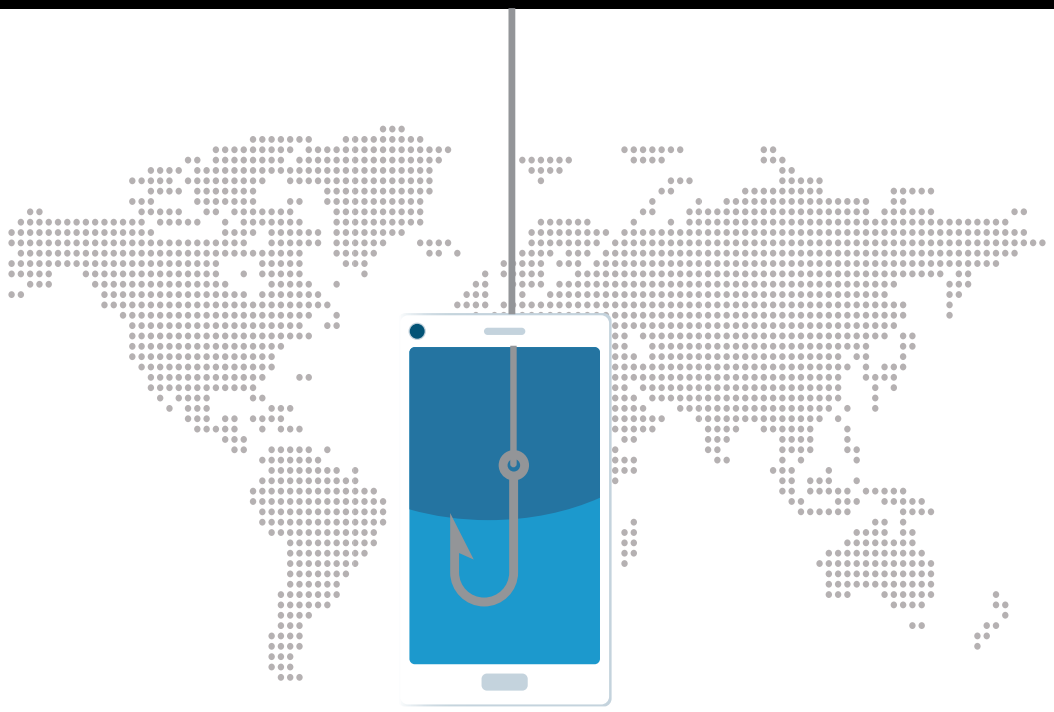
"Rarely does important data stay at rest", as Brown University[12] aptly phrases it. Given pandemic-related distributed workforce pressures, more data is throttling through cyber space than ever before. Once data departs a secure storage location, it is considered in-transit. At this point, it's uniquely vulnerable.

Is it more vulnerable than data at rest? Not necessarily. But it's vulnerable in different ways, and often times, organizations fail to take this into account. Once data is in-transit and has left your organization's network, you are no longer in control of it. Internal cyber security mechanisms cannot protect it.

In-Transit Threats

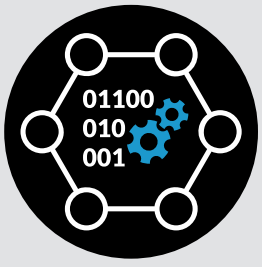
Data in-motion is vulnerable to man in the middle (MiTM) threats. Cyber adversaries could also intercept data using certain types of certificates, or they could embed 'sniffing' tools in your network.

12 "Data in Motion: Sending & Sharing Data," by Brown University.



Keeping Up With Regulatory Requirements

Data in-motion is subject to an ever-expanding list of regulatory guidelines. Presently, these are embedded in PCI, DSS, DPR, HIPAA, and SOX requirements. In complying with regulations, be sure to identify all of your in-motion data that remains at-risk. Lack of protections can lead to serious business consequences, ranging from heavy fines to litigation, as noted earlier. Regardless of the 'who, what, when, why and where', protections for in-transit data are critical.



Encryption can safeguard data in-transit. Encrypted data cannot be easily intercepted by Man-in-the-Middle attackers. In addition, consider a suite of security tools that include encryption, tracking and management of removable devices. When encryption tools are centrally managed, organizations receive unmatched control of policies, they can minimize the tools' impact on users, and organizations benefit from overall reductions in expenses.

Mitigate Epidemic Levels of Cyber Anxiety

Implementing a single solution to safeguard systems from cyber attack is futile. Cyber adversaries can easily circumvent a single roadblock. Organizations must pursue a strategic, multi-pronged approach.

Resolve the complexities and shortcomings of your current architecture. Look to leading cyber security vendors, like Check Point, for ideas and infrastructure options. You need layered, automated, and multi-modal protection to face today's advanced threats.

Talk to your Check Point sales representative for further information or reach out to sales@checkpoint.com. For more news and insights expertly tailored for senior security executives, visit CyberTalk.org.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com