Protect Your Business from Cyber Intrusions

Covid-19 has created an ideal environment for cybercriminals to attack corporate IT infrastructure. Find out how IT departments can withstand cyber intrusions.

Formaspace built these custom surveillance workstations in bright orange and black. Each unit supports 6 display monitors, and the worksurface provides ESD protection to prevent accidental damage to electronic equipment.

AUSTIN, TEXAS, UNITED STATES, October 6, 2020 /EINPresswire.com/ -- With many businesses closed to the public during the Covid-19 pandemic lockdown, online access has become a crucial economic lifeline, as millions of consumers have flocked to e-commerce websites and millions more have taken up working from home (WFH).

But this increased dependence on a reliable, robust online IT infrastructure carries its own costs.

According to the head of cybersecurity at CapGemini, worldwide spending on cybersecurity has reached $120 billion, and it's expected to grow to $300 billion by 2024. Yet, despite this enormous outlay, CapGemini estimates that worldwide losses due to cyber fraud totaled $2 trillion during 2019. Another consulting firm, Accenture, projects the cost of cyber fraud will rise to $5.2 trillion worldwide within five years.

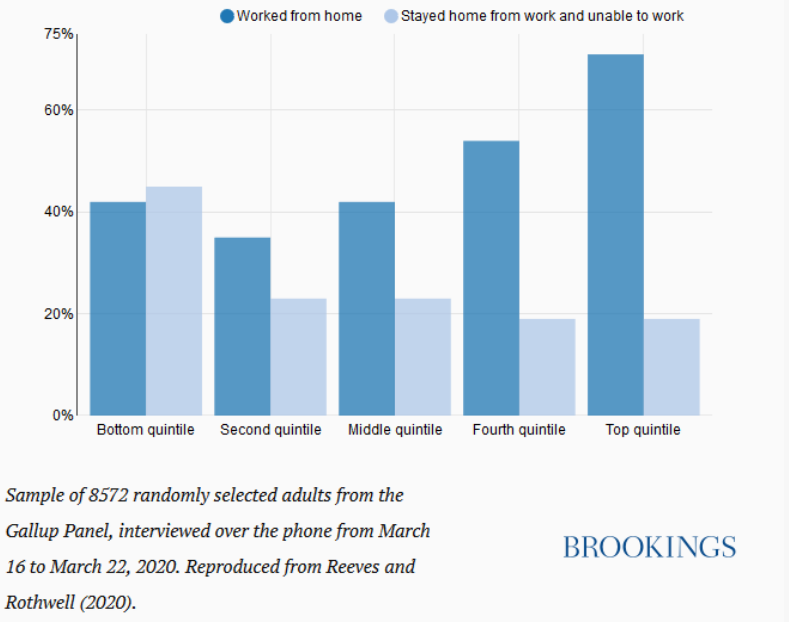
Over the years, many cyber-attacks have stayed on the down-low, to avoid public scrutiny for as long as possible. (Experts say creating a global standard for reporting cybercrime could help.)

But a series of high profile data breaches that put consumer data at risk has led to new governmental regulations obliging companies to come forward when customer data is exposed. The European GDPR (General Data Protection Regulation) is the most strict, penalizing companies with fines of up to 4% of annual turnover. (Fines for violating the new California

Consumer Privacy Act are less severe, at up to $7,500 per incident.)

For smaller companies, the cumulative costs of a cyber-attack could literally put them out of business – permanently. Insurance carrier Hiscox reports that each cyber intrusion costs businesses $200,000 on average, while Chubb calculates that the average cost for a business to recover from a cyber-attack is $400,000.

Compounding the financial risk is whether you can even make a cybersecurity insurance claim at all; many carriers are now arguing that attacks by so-called "state actors" should be considered as an "act of war" – a category excluded by most insurance policy riders.



Work from home has doubled during the pandemic, with nearly 75% of the highest earners working from home. Chart courtesy the Brookings Institute and Reeves and Rothwell.

How The Coronavirus Pandemic Has Increased Our Exposure To Cyber Crime

The Covid-19 pandemic has led to more employees working from home (WFM) as well as increased demand for e-commerce products and services, making this an ideal time for cyber criminals to attack corporate IT infrastructure.

> Covid-19 has led to more employees working from home, and increased demand for e-commerce products and services, making this an ideal time for cyber criminals to attack corporate IT infrastructure."
>
> *Formaspace*

Let's first take a look at the security implications of working from home.

A study from Reeves and Rothwell, cited by the Brookings Institute, found that the number of Americans working from home doubled during the pandemic lockdown.

Some tech companies (Twitter and Square, for example) are allowing employees to telecommute indefinitely, but, as we'll see in a moment, it's not a money-saving move as one might first believe. Companies have to expend significant resources, replicating the support employees would normally receive in the office, to meet the demand of home office workers accessing corporate data from potentially insecure equipment and locations.

Given these costs, it's no wonder that Facebook CEO Mark Zuckerberg believes that employees working from home will result in no net savings to his company: "The cost of supporting remote workers has generally offset the real estate and other costs of supporting people in the office," he said on a Facebook livestream. "There are just different costs here. Remote workers need different benefits in some cases, including things like more tooling to make their offices work at home."

With Formaspace custom furniture, home offices can be as functional and space-efficient as those found in traditional office buildings. This custom Formaspace office installation features natural maple hardwood work surfaces that wrap around the room.

What Are The Increased Cybersecurity Risks Associated With Working From Home

During the Covid-19 pandemic, cyber-attackers have been targeting employees working from home who are eager to learn about the latest virus news from legitimate organizations.

Numerous fake websites and fake emails purporting to be from legitimate sources have popped up during the pandemic. (Cybersecurity company Mimecast has a timeline showing how these scams have evolved during the pandemic.)

While the call to action (e.g. related to the Coronavirus) may be new, the underlying criminal intentions are generally the same: to steal corporate login credentials or capture credit card numbers (usually via phishing), trick users into downloading a secret Trojan software or other malware to their devices, or demand payment via ransomware, including a new variation, "sextortion," that threatens users with exposure of their supposed illicit web-visiting habits.

According to the FBI's 2019 Internet Crime Report, one particular kind of online fraud is especially costly.

Business Email Compromise (BEC), also known as Email Account Compromise (EAC), scams were responsible for over half of cybercrime losses in 2019 (over $1.7 billion, averaging $75,000 per complaint).

BEC/EAC scams are a relatively low-tech attack with the potential for a big payoff. In one type of BEC scam, hackers craft a legitimate-looking email account (or present fake invoices or wire transfer requests) and send it to unsuspecting individuals, companies, or government agencies.

The scam often fails, but when it hits, it can pay large dividends. For example, Galveston County in Texas paid over half a million dollars to a fake vendor posing as road paving contractor who requested a wire transfer payment be sent to a new bank account.

Like the FBI, the Internet Society has been tracking these scams; their most recent Cyber Incident & Breach Trends Report highlights these findings, which are broadly in line with the FBI's numbers:

Telecommunication provider Verizon also keeps track of cybercrime activity, and their most recent Data Breach Investigations report gives important insight into how the incident rates for the most common breaches have varied over the past 6 years.

According to Verizon, phishing tops the list for 2020, which should be especially worrisome for corporate IT security teams, as remote workers are potentially more vulnerable to these type of scams, as they often access a mix of home and business email from the same computer.

If they have not done so already, security teams need to implement end-to-end systems that can track corporate email and lock it down; they also need to teach their workers the importance of not clicking on imposter emails designed to capture their login credentials or other important data, such as banking information.

But email is not the only vulnerable type of software application. As has been widely noted, video conferencing and chat systems have suddenly become mission-critical tools for home-based workers trying to carry out their jobs. Yet, many of these popular communication and groupware apps have also been compromised, such as Zoom (which was plagued by so-called "Zoombombing" attacks prior to its recent end-to-end encryption upgrade) and Facebook's Whatsapp (which has become the target of a sophisticated spyware scheme.)

Risk To E-Commerce Providers Grow As Online Shopping Explodes During Lockdown

Just as the increase of people working from home has obliged corporate IT departments to step up their cyber surveillance activities to keep corporate data safe from cyber intrusions, e-commerce companies (and their various supply-chain partners) have also had to step up their game.

Read more...

Julia Solodovnikova
Formaspace
+1 800-251-1505
email us here
Visit us on social media:
Facebook

Twitter
LinkedIn
