CTM360®

Powered by **EDX LABS**


# THE CYBER FORECAST

## TOP 9 CYBERSECURITY THREATS FOR 2021

Technology advancements and disruptive ideas have forced organizations to embrace digital transformation; COVID-19 has only accelerated the same. Many organizations were not adequately prepared and this resulted in new challenges for the Cybersecurity industry during 2020. Looking forward at the cyber threat landscape of 2021, CTM360 sheds light on the Top 9 threats expected to stand out during the year.

# CYBERCRIME STATISTICS

The most recent 'SolarWinds' breach, a large scale supply chain attack continues to be unchartered territory where the full impact is still unknown. As in the past, empirical evidence from global cybersecurity incidents reveal a substantial increase in hacked and breached data. As the attack surface of organizations continue to grow with increased adoption of the cloud and third party vendors, more complexity has been added with increased usage of mobile and IoT devices in the workplace and at home. A big contributing factor is also increasing work from home and greater employee independence.

If it were measured as a country, then **cybercrime** which is predicted to inflict damages totaling **$6 trillion globally in 2021** would be the world's **third-largest economy** after the U.S. and China.

Cybersecurity Ventures expects global **cybercrime costs to grow** by 15 percent per year over the next five years, **reaching $10.5 trillion annually by 2025, up from $3 trillion in 2015.**

**- Cybersecurity Ventures**

The worldwide **information security market** is forecasted to **reach $170.4 billion in 2022**.

**- Gartner**

Malicious **hackers** are now attacking computers and networks at a rate of one **attack every 39 seconds.**

**- University of Maryland**

**71%** of **breaches** were financially motivated, & **25%** were motivated by espionage.

**- Verizon**

**68%**
of business leaders feel their **cybersecurity risks** are increasing.

**- Accenture**

**52%** of **breaches** featured hacking, **28%** involved Malware, and **32–33%** included Phishing or Social Engineering, respectively.

**- Verizon**

Cybercrime spend include but are not limited to damage and destruction of data, stolen money, stolen intellectual property & personal data, embezzlement, post-attack disruption, restoration and deletion of hacked data and systems, and reputational harm. **Despite increasing investment in cybersecurity globally, cybersecurity losses continue to rise exponentially.**

# 1 SPIKE IN RANSOMWARE ATTACKS

In ransomware attacks, cybercriminals steal or encrypt an organization's information and demand a ransom. If the organization refuses to pay, attackers threaten to publicly release or permanently delete the data, which forces the organization to choose between settling a large ransom or bearing the large scale reputational and financial loss.

**Global research predicts that businesses will fall victim to ransomware attacks every 11 seconds in 2021 compared to every 14 seconds in 2019.**

**THE ESTIMATED COST OF RANSOMWARE TO BUSINESSES WILL TOP $20 BILLION IN THE UPCOMING YEAR WITH AN AVERAGE ATTACK COSTING OVER $4 MILLION.**

One of the leading causes of this surge is that businesses have less tolerance for downtime with remote work. The lack of cybersecurity governance over remote work motivates threat actors further. It is increasingly common for breached organizations to pay ransom instead of the far more expensive post-attack remediation cost to avoid prolonged downtime, regulatory oversight, and minimize reputational damage in the public. The success of ransomware attacks encourages cybercriminals to continue this practice.

*Ref: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/*

*"The average downtime due to a Ransomware attack was 19 days in Q3 of 2020 compared to 12.1 days in Q3 2019."*

*- Coveware*

*"In 2019-2020, the average global cost to remediate a Ransomware attack was $761,106."*

*- Sophos*

*"The average cost of downtime is 24 times higher than the average ransom amount."*

*- Datto*

## 2 BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) is one of the most financially damaging online crimes. It exploits the fact that most organizations rely on email to conduct business. In a BEC scam, cyber-criminals send an email that appears to come from a legitimate source. After active reconnaissance on the victim's mailbox, these emails are sent to make financial requests that are timed perfectly and appear legitimate. BEC can be carried out using numerous tactics and techniques. One of the popular approaches is executive impersonation, also known as CXO Fraud.

In this scenario, the scammer assumes the personality of a high ranking executive. This tactic gives the victim a sense of urgency and persuades them to make the requested funds transfer/data disclosure with less probability of questioning the matter. One of the increasing trends to counter BEC is the correct implementation of DMARC, especially in financially sensitive sectors. Increased staff awareness and training is a high-value investment to avoid BEC.

*"$44,000 – the average cost for a Business Email Compromise hack."*

*- Verizon*

There has been a spike in BEC Fraud cases, increasing by 15% from Q2 to Q3 of 2020 - Abnormal Security

*Ref: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes*

## 3 BRAND ABUSE

The modern organization is evolving rapidly with increased cloud adoption and a greater digital presence. Accelerated by the pandemic, a majority of infrastructure and services have shifted online. Organizations are more focused on their online presence and are relying on it to conduct business. Brand abuse and brand impersonation will see a huge spike in the coming year as people rely more and more on online services.

**These attacks include impersonation on social media, job scams, next of kin scams, investment scams, fake news, and even to launch malware. With such a high variety of attack types, a new industry category dubbed Digital Risk Protection is rapidly evolving.**

**Beyond banking, finance, insurance and healthcare sectors, it is noted that online delivery services were highly targeted in 2020. Amazon and DHL were two of the most impersonated brands in 2020. It is expected that similar courier and delivery scams will increase in 2021. Brand oriented attack types also serve as launchpads for spear phishing and social engineering attacks.**

*"83% of Spear Phishing Attacks Involve Brand Impersonation."*

*- Barracuda*

# 4 SUPPLY CHAIN ATTACK

Supply chain attacks are cyber attacks that compromise a target organization by penetrating a third party vendor of software package instead of the organization itself. This style of attack proves especially lucrative to attackers for several reasons; a breach on one vendor creates a ripple effect which can have a much higher impact on all organizations downstream. During 2020, there has been an increased reliance on third parties to counter limited business and engineering resources. In addition, threats are often overlooked as organizations tend to trust the vendors they use in day to day business.

**The biggest supply chain attack of 2020 was the SolarWinds hack where attackers pushed malicious code as part of an update package of the Orion software. This affected 18000+ customers of SolarWinds which including Microsoft, Cisco, Intel, and multiple US government agencies. In 2020, experts have warned of a 430% increase in supply chain attacks targeting open-source tools used across industries. These figures are expected to increase further in 2021 as organizations are deploying more third-party services and tools to facilitate their operations.**

> *"63% of all cyber-attacks could be traced either directly or indirectly to third parties."*
>
> *- PwC*

Usually IT vendors or small businesses are the perfect entry point for hackers since they lack security controls. Organizations should evaluate the cybersecurity posture of all their third-party vendors to eliminate the risk of supply chain attacks.

*Ref: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12*

# 5 ATTACKS ON RDP/VPN

With increasing remote activity, many organizations have been implementing Remote Desktop Protocol (RDP) & Virtual Private Networking (VPN) to allow access to corporate data and servers off-site. Although RDP is already one of the most commonly attacked services online, the next year is expected to see a further spike in exploitation of RDP, VPN, and other remote services.

Despite the additional security layer that VPN provides, cybercriminals view VPN as an open gateway into an organization's entire network if access is achievable. **As data breaches increase, cybercriminals have an abundance of leaked credentials paired with exploits and brute force opportunities; thus almost doubling the attacks against RDP, VPN, and remote connection servers in 2021.**

> *"RDP Brute-force Attacks grew 400% in March and April alone."*
>
> *- Kaspersky*

*Ref:https://www.csoonline.com/article/3542895/attacks-against-internet-exposed-rdp-servers-surging-during-covid-19-pandemic.html*

# 6 DATA BREACHES ON CLOUD-BASED INFRASTRUCTURE AND SERVICES

Cloud adoption has its own challenges. Organizations are expected to implement their own cybersecurity infrastructure and configure them adequately to secure themselves. Infrastructure as a Service (IaaS) vendors typically have a shared security services model. Subsequently, misconfigurations may lead to data breaches and exposure of sensitive corporate information; this is a high risk.

This risk gives rise to 3 major challenges.

- **Employees do not have adequate skills and knowledge in cloud security and hence it leaves an open door for hackers.**
- **The current security frameworks lack adequate mapping to implement security measures on cloud services and this exponentially increases the risk.**
- **Exposure of mission critical or corporate data left exposed on the internet for attackers to access.**

The most common misconfiguration is over-privileged user accounts. When attackers gain access to an associated identity with broad privileged permissions, they can abuse those permissions maliciously.

*"Number of records exposed reaches a staggering 36 billion in 2020."*

*- Risk Based Security*

*“Errors caused 22% of Data Breaches.”*

*- Verizon*

*“82% of cloud users have experienced security events caused by confusion over who is responsible to secure the implementations.”*

*- Oracle and KPMG*

# 7 DATA EXPOSURE ON CODE REPOSITORIES

Developers routinely use code repositories such as GitHub to back up, share, and manage changes to code. It is a popular environment for collaborative development by the developer community; however, code repositories are also public by default, which means that anyone can find and access code that has been uploaded to such websites.

**And all too often, developers forget to remove sensitive data from their code or make the repositories private before uploading them on GitHub. Malicious hackers actively scan and scrape GitHub for leaked passwords, client IDs, secret keys, and API tokens, to name a few, because they know programmers are prone to such oversight.**

With the current rise in remote work, development teams are often scattered, working remotely and sharing code via online repositories. Data exposure risks will subsequently increase with limited security governance and lack of practical controls.

*Ref: https://unit42.paloaltonetworks.com/github-data-exposed/*

> *"Unit 42 researchers analyzed more than 24,000 public GitHub data uploads via GitHub's Event API and found thousands of files containing potentially sensitive information, which included: 4109 Configuration files, 2464 API keys, 2328 Hardcoded username and passwords, 2144 Private key files, 1089 OAuth tokens."*
>
> *- Palo Alto*

# 8 TARGETED THREATS LEVERAGING REMOTE WORK

New security challenges are brought on by the rapid deployment of tools, technologies, and processes that enable people to work remotely. The shift in working practices, associated devices, and locations makes it far easier for these types of threats to go unnoticed. The rapid increase of mobile devices widens the organization's potential attack surface. This threat is further amplified by the associated rise in cloud adoption and the short-term 'Use Your Own Device' (UYOD) policies that many organizations adopted to overcome remote work challenges.

**Employees working from home use devices that aren't patched, managed, or secured by the corporate IT department. This gives hackers an entry point into the network that bypasses the perimeter security. Sensitive company data is being stored on these devices, further increasing the risk of data breaches.**

Additionally, the majority of people do not manage the default settings of their home router which leaves an entry point for hackers to access the network and confidential data. Moreover they may have many IoT devices within their home network with inadequate security controls which can also prove to be a threat.

> *"In corporate contexts, decision-makers are aware of the issue: 83% of them said that their organization was at risk from Mobile Threats and 86% agreed that Mobile Threats are growing faster than others."*
>
> *- Verizon*

# 9 PHISHING, VISHING, AND SMISHING ATTACKS

Since its outbreak in March 2020, COVID-19 has been the main headline of news and media outlets. Threat actors recognized this pandemic as the most apparent bait to make their schemes more effective. The use of the COVID-19 pandemic as a theme for phishing campaigns is expected to progress into 2021. Attacks will often coincide with significant events or news, such as a spike in new cases or a new vaccine drug's announcement.

Smishing and Vishing attacks are also growing as cybercriminals turn to mediums that are trusted more than email. Smishing is a type of social engineering attack that utilizes SMS text messaging as its medium. Vishing, on the other hand, is conducted via phone calls. There is no current filter or technology where numbers are confirmed as trusted sources, making mobile phone users more vulnerable to these attacks.

**There are different variations of these campaigns.**

**For example, impersonating official healthcare entities like the WHO, hospitals, and insurance companies is a prevalent pattern. Another variation that scammers opt for is masking as relief funds and donation campaigns.**

**Other than attacks directly connected to COVID-19, a rise in activity related to the after effects of the pandemic is anticipated. These may include fictitious employment opportunities, investment propositions, threats to online collaboration activities, and various online shopping scams.**

*"According to Verizon's 2020 Mobile Security Index, Smishing Attacks have increased from 2 percent to 13 percent in just the past year."*

*- Verizon*

*"More than 60% of Phishing Attacks involve keyloggers."*

*- Cofense*

*"A single Spear-Phishing Attack results in an average loss of $1.6 million."*

*-Security Boulevard*

*"In Q3 of 2020, APWG detected almost 572,000 unique Phishing websites and observed more than 367,000 unique Phishing email subjects."*

*- APWG*


## YOUR CYBERSECURITY TEAM IN THE CLOUD

CTM360® is a 24 x 7 x 365 Cyber Security subscription service for detecting and responding to cyber threats. Headquartered in the Kingdom of Bahrain, CTM360 specializes in offensive defense and strives to strengthen the security posture by making you harder target in cyberspace.

To learn more about CTM360,

**visit: www.ctm360.com | Email: Info@ctm360.com**