HISCOX
CYBERCLEAR®

TOP FIVE CYBER RISKS IN 2021

The global cyber risk landscape quickly shifted in 2020, affecting businesses across all sizes and sectors. The impact of COVID-19 was felt with increased phishing email success in March; however, it also heightened awareness of cyber risks for both consumers and businesses.

At the end of 2019, the first instance of ransomware gangs threatening to publish exfiltrated data occurred. This evolution of ransomware into doxing, or the publishing of stolen data, means ransomware attacks are now also data breaches. Now, more costs will be incurred and it will take longer to recover. Legal action across the USA and UK has increased as fallout from the proliferation of data breaches, mostly due to business email compromise (BEC) and ransomware/doxing.

Open remote desktop protocol (RDP) ports, lack of patching, and virtual private network (VPN) vulnerabilities were major causes of ransomware in 2020. Over the summer, Microsoft released over a hundred vulnerabilities a month, requiring a massive patching effort that could leave businesses vulnerable.

Major supply chain breaches in the fall and winter – Blackbaud and SolarWinds – took over headlines as global companies and nearly every US government branch were affected. The full scope of both attacks continues to unfold.

So what's next? The most important takeaway of 2020 is that it's imperative businesses take cyber security seriously. Certain trends are here to stay and businesses of all sizes must protect, stay vigilant, and build resilience.

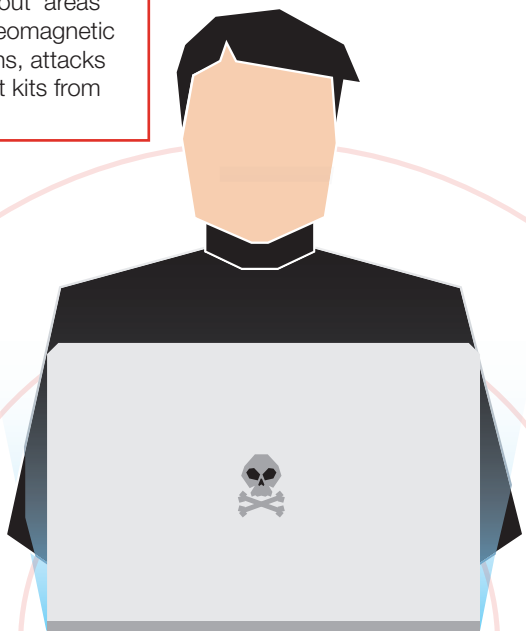
Continued COVID-19 threat
Phishing campaigns will move from COVID-19 spread to vaccine information and sign-up. Attacks will likely target the COVID-19 response effort and corresponding industries and services – healthcare, local government, vaccine distributors, etc.

Legal landscape shifts
Third-party and class action lawsuits, along with GDPR/regulatory fines, will increase as data breaches grow because of doxing and supply chain attacks. Given the pressure of ransomware, we'll likely see further government intervention and policy changes surrounding ransomware payments and prevention requirements.

New attack vectors
We need to think as creatively as cyber criminals, anticipating their moves. Potential 'watch out' areas include – point of sale malware attacks, geomagnetic storms and other electromagnetic weapons, attacks on time protocols, and weaponized exploit kits from nation states.

Evolution of ransomware
Criminals are creative and innovative when it comes to putting pressure on victims to pay. Various attack vectors will be used in conjunction to cause further disruption – DDoS and doxing on top of ransomware. Open RDP ports and exploitation of remote access vulnerabilities will continue to be key avenues of entry for cyber criminals. Doxing poses may cause major costs to all businesses and the cyber insurance industry at large.

SolarWinds fallout
Immediate impacts and broad ramifications still unknown. Potential copycat attacks likely, leveraging software supply chains as targets. Build and deploy services have always been built for speed and convenience, not security. Be wary of exploitation of critical vulnerabilities in Microsoft and other digital services products.



21420 02/21