WINTER 2021 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, cybersecurity and data analytics needs. For this E-Newsletter, we focus on data leakage and organizational risk, as well as cybersecurity trends for 2021.

Top Ten Cybersecurity Trends to Watch in 2021

With the welcome arrival of the COVID-19 vaccine coinciding with the departure of the year 2020, individuals and organizations are anticipating what they can expect in 2021. Digital Mountain is no exception – already tracking what we expect to see in 2021. In addition to employees returning to office environments, businesses re-opening their doors, and the economy regaining strength, we're tracking some eye-opening cybersecurity trends that could potentially influence 2021 in interesting ways, and we'd like to share those with you.

1. **Distributed Network Information Security is here to stay.** Whether your organization is continuing to encourage remote work or just making access to data flexible, securing data wherever and whenever is an issue that will continue to evolve in 2021. The challenge to secure data being accessed remotely rose quickly in 2020 and required rapid responses that often resulted in expediency at the cost of thorough design and implementation of best practices. 2021 should see the re-alignment of remote access with tighter data security.
2. **IT talent, including C-suite management, will continue to see their statures rise.** With cybersecurity firmly ensconced as a priority for organizations, IT personnel, especially those in director and officer positions will becoming increasingly valuable to forward thinking organizations. As a result, whatever your core business or services, be prepared to face labor constraints in finding and even potentially retaining competent and experienced IT staff and management. Establishing relationships with outside vendors who can step in at a moment's notice will help mitigate IT disruptions for your organization.

3. **Increasing demand for Auxiliary Cybersecurity Services.** If you haven't come to this conclusion already, we're happy to give you the heads up: Cybersecurity services are going to be in high demand in 2021. For all the reasons we've stated above, and those below, organizations will look to outside experts for training, security assessments, penetration testing, security audit preparation, managed services, etc. with greater frequency to provide comprehensive cybersecurity solutions in 2021. Proactive organizations will consider both reserving budget allotments and establishing relationships with professional cybersecurity providers, such as Digital Mountain, to stay ahead of the demand.
4. **Cloud Security storms are brewing.** Again, the rapid migration to remote work capability may have created inadvertent lapses or holes in cybersecurity which will need to be addressed in 2021 or organizations will realize exposure from those risks. Many organizations that relied upon the security measures of cloud services to protect data will now back-track and reassess if those standard features provide adequate protection or if increasing security is a prudent course.
5. **Insider Threats recognized for the danger they present.** We know that disgruntled employees with legitimate access to data can do vast damage, as can careless employees who either misuse data privileges or ignore best practices. Compromised employees, including executive-level employees, are also further becoming known as potential insider threats. 2021's focus on greater cybersecurity provides an opportunity to recognize and remediate threats from within an organization.
6. **Ransomware still looking for a victim.** An incredibly lucrative crime, ransomware isn't going away in 2021. In fact, with enhanced capabilities such as Distributed Denial of Service attacks lurking around in emails of unsuspecting victims, we anticipate ransomware will surge. Increased cybersecurity awareness and adherence to best practices, investment in services to detect and prevent damage from ransomware, and hopefully, a renewed commitment to not pay ransoms will help reduce the peril that cybercriminals present.
7. **AI and Big Data Analytics are marrying up for cybersecurity.** AI garnered a lot of press in 2020 – deepfakes, modeling advancements in the Coronavirus spread, increasing the accuracy of algorithms, even generating social media posts and longer pieces of writing. Now, we can look forward to AI and big data analytics coming together on behalf of cybersecurity by increasing the speed, depth, and effectiveness of network traffic analysis to predict and identify threatening activity.
8. **Zero-Trust Networks gain trust.** While Virtual Private Networks (VPNs) have taken centerstage in 2020 to help thwart cybercrime, VPNs subscribe to a long-held belief that cybersecurity is about keeping out bad actors while allowing trusted users to work as unimpeded as possible inside the network. Zero-Trust Networks call out that exterior defense/interior accessibility model as flawed and advocate for a trust no one approach when it comes to cybersecurity. Zero-Trust Networks invoke multifactor authentication, ubiquitous encryption, strict permission rules, and least-access policy adherence, as well as network segmentation, to increase organization-wide security from both internal and external threats. This shift in network design may require a strategy pivot for organizations, but the enhanced security it provides may well be worth the effort.

9. **Creeping Toward Legislation.** According to the National Conference of State Legislatures, almost 300 pieces of legislation pertaining to cybersecurity were introduced in 2020, many of which were left on the table while governments turned their attention to deal with the Coronavirus pandemic (https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx). The many data breaches, hacking events, and various other cybersecurity concerns of 2020 should reinvigorate the push to increase the penalties for cybercrimes, as well as up the requirements of organizations collecting and storing data to behave responsibly in protecting data. We know that legislative efforts often lag compared to technology development, but one benefit of government efforts to create cybersecurity legislation is that overall attention appears to increase.

10. **Bad Actors will continue to behave badly.** In the wake of the SolarWinds hack revealed in early December 2020, our attention was again taken up with the story that nation-state bad actors continue to target governments and organizations storing data sought after by those seeking to gain a financial and/or political advantage. While not all of the purported 18,000 clients impacted by the SolarWinds hack will be impacted to the same extent (https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm), what we can extrapolate is that the sophisticated methods used successfully to insert malicious code into a trusted product are not likely to be abandoned anytime soon. These professional hackers are likely to continue playing a long-game with powerful interests backing them up. What's an organization to do? Keep a careful eye on data, adhere to best practices, and be ready to respond with help from experienced professionals.

While no one can accurately predict the future, we're betting these ten trends, and many more, will have significant impact on 2021's cybersecurity environment. Digital Mountain is prepared to help your organization take on whatever the new year brings, and we're resolved, as we hope you are, that 2021 will be the year that we leave the worst cybersecurity issues of 2020 behind. Happy New Year from Digital Mountain!

Please direct questions and inquiries about electronic discovery, computer forensics, cybersecurity and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

ALA MIDWINTER MEETING & EXHIBITS, VIRTUAL
January 22-26, 2021

PLI GOVERNMENT INVESTIGATIONS 2021: INVESTIGATIONS ARISING FROM DATA BREACH AND PRIVACY CONCERNS AND PARALLEL PROCEEDINGS, VIRTUAL
January 27, 2021

EDRM EXPOCOM 2021

February 1-3, 2021

LEGALWEEK VIRTUAL SERIES 1
February 2-4, 2021

TECHSHOW 2020, VIRTUAL
March 8-13, 2021

Click here to see more upcoming events and links.

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com. In the short term, she is available for webinars and remote e-conferences.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: