With corporate cybersecurity breaches becoming more and more commonplace, and with threats and fines mounting as we become increasingly reliant on cloud-based computing and other online innovations, cybersecurity is now more important than ever.

With hundreds of thousands more employees working from home, and devices containing sensitive data leaving offices and entering homes at an exponential rate, data security concerns have exponentially increased.

While tools to prevent breach incidents have become more sophisticated, so have the methods of the hackers and cybercriminals.

This special supplement to the San Fernando Valley Business Journal collects some guest articles and news exploring the latest trends and tips to keep our businesses and our customers safe from cyber-attacks, hacks and breaches.
Top Security and Risk Management Trends for 2021

Security and risk management leaders must address eight top trends to enable rapid reinvention in their organization, as COVID-19 accelerates digital business transformation and challenges traditional cybersecurity practices, according to Gartner, Inc.

In the opening keynote at the Gartner Security & Risk Management Summit taking place virtually in APAC last month, Peter Firstbrook, research vice president at Gartner, said these trends are a response to persistent global challenges that all organizations are experiencing.

“The first challenge is a skills gap. 80% of organizations tell us they have a hard time finding and hiring security professionals and 71% say it’s impacting their ability to deliver security projects within their organizations,” said Firstbrook.

Other key challenges facing security and risk leaders in 2021 include the complex geopolitical situation and increasing global regulations, the migration of workspaces and workloads off traditional networks, an explosion in endpoint diversity and locations and a shifting attack environment, in particular, the challenges of ransomware and business email compromise.

The following top trends represent business, market and technology dynamics that are expected to have broad industry impact and significant potential for disruption.

**TREND 1: CYBERSECURITY MESH**
Cybersecurity mesh is a modern security approach that consists of deploying controls where they are most needed. Rather than every security tool running in a silo, a cybersecurity mesh enables tools to interoperate by providing foundational security services and centralized policy management and orchestration. With many IT assets now outside traditional enterprise perimeters, a cybersecurity mesh architecture allows organizations to extend security controls to distributed assets.

**TREND 2: IDENTITY-FIRST SECURITY**
For many years, the vision of access for any user, anytime, and from anywhere (often referred to as “identity as the new security perimeter”) was an ideal. It has now become a reality due to technical and cultural shifts, coupled with a now majority remote workforce during COVID-19. Identity-first security puts identity at the center of security design and demands a major shift from traditional LAN edge design thinking.

“The SolarWinds attack demonstrated that we’re not doing a great job of managing and monitoring identities. While a lot of money and time has been spent on multifactor authentication, single sign-on and biometric authentication, very little has been spent on effective monitoring of authentication to spot attacks against this infrastructure,” said Firstbrook.

**TREND 3: SECURITY SUPPORT FOR REMOTE WORK IS HERE TO STAY**
According to the 2021 Gartner CIO Agenda Survey, 64% of employees are now able to work from home. Gartner surveys indicate that at least 30-40% will continue to work from home post COVID-19. For many organizations, this shift requires a total reboot of policies and security tools suitable for the modern remote workspace. For example, endpoint protection services will need to move to cloud delivered services. Security leaders also need to revisit policies for data protection, disaster recovery and backup to make sure they still work for a remote environment.

**TREND 4: CYBER-SAVVY BOARD OF DIRECTORS**
In the Gartner 2021 Board of Directors Survey, directors rated cybersecurity the second-highest source of risk for the enterprise.

“80% of organizations tell us they have a hard time finding and hiring security professionals and 71% say it’s impacting their ability to deliver security projects within their organizations.”

Gartner predicts that by 2025, 50% of large organizations will adopt privacy-enhancing computation for processing data in untrusted environments or multiparty data analytics use cases.

**TREND 5: SECURITY VENDOR CONSOLIDATION**
Gartner’s 2020 CISO Effectiveness Survey found that 78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio; 12% have 46 or more. The large number of security products in organizations increases complexity, integration costs and staffing requirements. In a recent Gartner survey, 80% of IT organizations said they plan to consolidate vendors over the next three years. “CISOs are keen to consolidate the number of security products and vendors they must deal with,” said Firstbrook. “Having fewer security solutions can make it easier to properly configure them and respond to alerts, improving your security risk posture. However, buying a broader platform can have downsides in terms of cost and the time it takes to implement. We recommend focusing on TCO over time as a measure of success.”

**TREND 6: PRIVACY-ENHANCING COMPUTATION**
Privacy-enhancing computation techniques are emerging that protect data while it’s being used — as opposed to while it’s at rest or in motion — to enable secure data processing, sharing, cross-border transfers and analytics, even in untrusted environments. Implementations are on the rise in fraud analysis, intelligence, data sharing, financial services (e.g. anti-money laundering), pharmaceuticals and healthcare.

Additional information is available at gartner.com.
Work From Home Cybersecurity Tips

By following a few simple best practices, even novice remote workers can do their part to keep themselves and their companies safe while working from home. Below, the cybersecurity experts at MonsterCloud review some work-from-home cybersecurity tips that will help lessen the chance that an employee or their company will fall victim to cybercrime.

COVID-19 INCREASES CYBERATTACKS

Since the pandemic began and the majority of people’s lives was forced online, cybercrime has soared. The Cyber Division of the FBI recently released incredible statistics on what they are seeing during the pandemic. At one point, the division was getting up to 4,000 complaints of cyberattacks a day. That number is a 400% increase from the number of complaints before the pandemic started.

It is not just a U.S. issue either. The European-based international police organization, Interpol reports that “with organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption.”

These statistics and statements both point to the same thing. Cybercriminals are taking advantage of the fact that people are working from home and using that to their advantage. They are using ransomware, phishing scams, malware, and more to gain access to companies’ systems for profit.

WHO ARE CYBERATTACKERS TARGETING?

The short answer is, ransomware attackers will attack anyone with a computer and an internet connection without thinking twice about it. Big companies, small businesses, nonprofits, municipalities, and even individuals are all seen as potential targets. This is a crime designed to make the criminals money so the more people and organizations they attack, the more money they have that their ransom will be paid.

That said, there are institutions that these criminals are attacking at a much higher rate and with much more intensity than others. Right now, because of how hectic these organizations are due to the coronavirus and how many people have - many of whom are working from home - these places are more susceptible to attacks than others. This includes large, multinational companies, the healthcare, industry, schools, and local governments.

RECENT ATTACKS

No one can be sure from the outside that all the recent, major cyberattacks are due to working at home. Only when a skilled cybersecurity company like MonsterCloud reviews the attack can the true source of the attack be found. However, the sheer increase in successful attacks paired with the COVID-related stay-at-home orders makes it a good bet that the two things are related.

MONSTERCLOUD REVIEWS TOP CYBERSECURITY TIPS

• Tip #1: Make Sure Systems are Up to Date

Still hitting “Remind Me Tomorrow” on that system update prompt the computer has been reminding about since the pandemic started? If so, it’s way past time to install any updates that are needed.

• Tip #2: Make Sure Anti-Virus Software is Up to Date

The tip is to keep anti-virus software up to date, but that is assuming the software is being used. If not, stop reading this right now and go install one. Anti-virus software is the easiest way to protect from hackers. Like in most situations, the criminals will always be ahead of the people trying to stop them but anti-virus software will catch the majority of attacks before they harm the system.

• Tip #3: Watch Out for COVID-19 Phishing Scams

When MonsterCloud reviews the ransomware attacks that have happened during the pandemic, the company has found that many have started with pandemic-related phishing emails. These emails are designed to take advantage of people’s curiosity and thirst for knowledge about pandemic-related topics.

• Tip #4: Watch the Wireless Internet

Whether logging onto the internet-based cloud or a company’s in-house servers to access the company’s systems, chances are people are using WiFi to do so. Securing WiFi’s is of critical importance when working from home. If the home WiFi is not password protected, that is something that needs to be done. If it is, make sure that the password is a strong password and not the default one the router came with. Using something like an address or “password123” is not a good idea.

Cybercrime, especially ransomware, is a huge problem right now. The global pandemic has forced people to work from home and criminals are taking advantage of this with a growing number of attacks. By following these few simple tips though, everyone can be better prepared to work from home and have less of a chance of being the cause of a cyberattack on their company.

Information for this article was provided by MonsterCloud. Learn more at monstercloud.com.
Cybersecurity and Communication Lead 2021’s Top Five Technology Trends

Pandemic also advances collaboration, edge computing, and outsourced IT departments

Information technology (IT) underwent a major change in 2020 as organizations were forced to quickly adopt strategies to handle new cybersecurity threats and increased remote working and collaboration needs, according to Matrix Integration, a strategic IT solutions and managed services provider for more than 1,000 businesses and schools in the Midwest and beyond. “Cybersecurity remains a top concern for 2021, as hackers continue to threaten organizations, particularly in energy, utilities, government, and manufacturing,” said Reggie Gresham, vice president of sales and marketing at Matrix. “The work we’ve done includes new cameras, endpoints, additional bandwidth, and easy-to-use software tools to facilitate all kinds of collaboration and e-learning scenarios.”

For 2021, Matrix Integration has predicted that organizations will continue or increase their investment in these top five areas:

1. **Cybersecurity.** A different approach to cybersecurity in 2021 may be necessary. For example, consulting firm Accenture estimates that while direct attacks may have fallen, indirect attacks to supply chain and infrastructure are on the rise, causing organizations to broaden their approach to thwarting cyberattacks.

2. **Enterprise-level telephony systems for any business.** With the increase in cloud-based services, small- and medium-sized businesses (SMBs) can now have the same level of sophisticated phone services as major enterprises. The size of the system is easily managed and can be scaled up or down. Advantages include no capital investments or aging hardware and simplified management and control. As remote work will likely continue into 2021 and beyond, IP-based phone systems make it easy for employees to connect from anywhere.

3. **Unified Collaboration.** The ability to work together across applications is both a short- and long-term goal that many of Matrix’s clients have embraced for 2021. In 2020, together with Cisco, Matrix Integration deployed a wide variety of easy-to-use technologies for individuals and teams, including content sharing, encryption of sensitive data, and cutting-edge, cloud-based phone systems that all work together seamlessly.

4. **Edge-to-Cloud.** More than 30 percent of essential applications and data live in hardware-based data centers. Instead of moving these systems to the cloud—an expensive and time-consuming undertaking—new technologies now move the cloud to the edge. Working with ITE GreenLake, Matrix Integration can bring cloud services to these data centers, allowing users to deploy services such as artificial intelligence and machine learning, as well as add speed and agility to on-the-ground information.

5. **Virtual IT Departments.** Many small- and medium-sized businesses are realizing that outsourcing their IT departments altogether generates a significant ROI. In 2020, Matrix Integration worked with a growing number of clients to implement a Managed Services contract, with companies handing the reigns over to Matrix to handle IT issues ranging from routine user questions to cybersecurity maintenance and data backups. In addition to reducing the total cost of ownership, outsourcing expands IT capabilities for businesses, providing them with additional tools and services that they may otherwise not have access to.

Cybersecurity Study Highlights Imperatives for State Governments

Continued need for cross-boundary collaboration and increased modernization and digital government services brought to light by COVID-19

Last October, Deloitte and the National Association of State Chief Information Officers (NASCIO) released their 2020 Cybersecurity Study, “Cybersecurity and Communication Lead 2021’s Top Five Technology Trends.” The report also details focus areas for states during the COVID-19 pandemic. While the pandemic has highlighted the resilience of public sector cyber leaders, it has also called attention to long-standing challenges facing state IT and cybersecurity organizations such as securing adequate budgets and talent; and coordinating consistent security implementation across agencies. These challenges were exacerbated by the abrupt shift to remote work spurred by the pandemic.

According to the study:

*Before the pandemic, 52% of respondents said less than 5% of staff worked remotely.*

*During the pandemic, 35 states have had more than half of employees working remotely; nine states have had more than 90% remote workers.*

Recent times have created new opportunities for cyber threats and amplified existing cybersecurity challenges for state governments,” said Meredith Ward, director of policy and research at NASCIO. “The biggest talent challenges experienced in recent years have only grown, and CISOs are now also faced with an acceleration of strategic initiatives to address threats associated with the pandemic.”

The pandemic forced state governments to act quickly, not just in terms of public health and safety, but also with regard to cybersecurity, said Srini Subramanian, principal, Deloitte & Touche LLP, and state and local government advisory leader. “However, continuing challenges with resources beset state CISO/CIOs. This is evident when computing the much higher levels of budget that federal agencies and other industries like financial services receive to fight cyber threats.”

State governments’ longstanding need for digital modernization has only been amplified by the pandemic, along with the essential role that cybersecurity needs to play in this discussion. Key takeaways from the 2020 study include:

- Fewer than 40% of states reported having a dedicated budget line item for cybersecurity.
- Half of states still allocate less than 3% of their total information technology budget on cybersecurity.
- CISOs identified financial fraud as three times greater of a threat as they did in 2018.
- Overall, respondents said they believe the probability of a security breach is higher in the next 12 months, compared to responses to the same question in the 2018 study.
- Only 27% of states provide cybersecurity training to local governments and public education entities.
- Only 28% of states reported that they had collaborated extensively with local governments as part of their state’s security program during the past year, with 65% reporting limited collaboration.

The 2020 study also revisits the three “bold plays” of the 2018 Deloitte-NASCIO Cybersecurity Study, covering funding, innovation and collaboration, to assess progress on these strategic issues. While CISOs have made progress in the intervening years, more is needed.

The study is based on responses from U.S. state and territory enterprise-level CISOs. The 2020 study revisits the three “bold plays” of the 2018 Deloitte-NASCIO Cybersecurity Study, covering funding, innovation and collaboration, to assess progress on these strategic issues. While CISOs have made progress in the intervening years, more is needed.

The study is based on responses from U.S. state and territory enterprise-level CISOs. The 2020 study revisits the three “bold plays” of the 2018 Deloitte-NASCIO Cybersecurity Study, covering funding, innovation and collaboration, to assess progress on these strategic issues. While CISOs have made progress in the intervening years, more is needed.

The study is based on responses from U.S. state and territory enterprise-level CISOs. The 2020 study revisits the three “bold plays” of the 2018 Deloitte-NASCIO Cybersecurity Study, covering funding, innovation and collaboration, to assess progress on these strategic issues. While CISOs have made progress in the intervening years, more is needed.
Cybersecurity & IT

Responsible Data Destruction Should be Priority #1

By JOHN SHEGERIAN

Data destruction should be on the top of every business’ “things to plan” list. If you have papers, storage devices, or electronic items that are no longer needed, you can’t just throw them away. You can’t ignore the importance of having professional data destruction steps in place. If you haven’t thought about how you handle end-of-life devices, you need to. Go back a little more than 10 years to 2010. At that point, data and information creation was at around 2 petabytes. A petabyte is a million gigabytes. Two trillion gigabytes is a lot of information. Now, skip forward to the end of 2020. In just 10 years, the creation of data and information has increased to an estimated 59 zettabytes. A zettabyte is a trillion gigabytes. Two trillion gigabytes is a lot of information.

WHERE IS YOUR DATA?

Any data containing your proprietary company information, your customers’ data or employees’ personal information must be secured. Before you dispose of old, unused electronics, professional data destruction is essential.

Don’t take the chance and destroy the data on your own. Chances are you’re not going to do it correctly. If someone steals information that wasn’t properly destroyed, not only do you face huge fines, but you also face damage to your company’s reputation.

Damage to a reputation is especially important to consider. It’s estimated that about 60% of small and medium-sized companies that are impacted by a data breach end up going out of business within six months. Partner with a professional data destruction firm and lower the risk of fines and lost business.

HOW MUCH COULD YOU PAY?

How much can companies pay in fines? It varies. If you manage medical records, improperly destroyed data can violate HIPAA. Fines for HIPAA violations can be as high as $1.5 million. Financial institutions are bound by the rules of the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act. While FCRA fines can be as high as $3,756 per violation, Gramm-Leach-Bliley Act violations come with penalties of up to $1.1 million. Here are some of the fines levied on companies that violated data destruction and e-recycling regulations.

Affinity Health Plan was ordered to pay fines of $1.2 million back for a 2010 case where the information of more than 344,000 people was found on copier hard drives that the managed care plan provider had leased. When they returned the leased copiers, the information had never been destroyed as per HIPAA rules.

From 2013 to 2015, hundreds of Home Depot stores were caught throwing away batteries, fluorescent light bulbs, paints, and unused electronics. These items were not only going illegally to area landfills, but it’s believed that some of the electronic devices may have contained customer information. The company was fined $18.5 million and also had to pay close to $10 million more to help with environmental projects and complying with other measures ordered by the courts.

Morgan Stanley learned the importance of proper data destruction. The company was fined $60 million for failing to have electronic data disposed of correctly during the decommissioning of two data centers. While they’d had a company helping with the decommissioning, they didn’t keep track of the data stored on the hardware or oversee where the hardware went. After one warning, the same incident happened several years later, so fines were issued.

HOW MUCH COULD YOU PAY?

How much can companies pay in fines? It varies. If you manage medical records, improperly destroyed data can violate HIPAA. Fines for HIPAA violations can be as high as $1.5 million. Financial institutions are bound by the rules of the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act. While FCRA fines can be as high as $3,756 per violation, Gramm-Leach-Bliley Act violations come with penalties of up to $1.1 million. Here are some of the fines levied on companies that violated data destruction and e-recycling regulations.

Affinity Health Plan was ordered to pay fines of $1.2 million back for a 2010 case where the information of more than 344,000 people was found on copier hard drives that the managed care plan provider had leased. When they returned the leased copiers, the information had never been destroyed as per HIPAA rules.

From 2013 to 2015, hundreds of Home Depot stores were caught throwing away batteries, fluorescent light bulbs, paints, and unused electronics. These items were not only going illegally to area landfills, but it’s believed that some of the electronic devices may have contained customer information. The company was fined $18.5 million and also had to pay close to $10 million more to help with environmental projects and complying with other measures ordered by the courts.

Morgan Stanley learned the importance of proper data destruction. The company was fined $60 million for failing to have electronic data disposed of correctly during the decommissioning of two data centers. While they’d had a company helping with the decommissioning, they didn’t keep track of the data stored on the hardware or oversee where the hardware went. After one warning, the same incident happened several years later, so fines were issued.

Sometimes, fines aren’t immediately proposed, but court-ordered actions are imposed. Australia’s Commonwealth Bank was found to have lost magnetic storage tapes containing records for upwards of 20 million bank customers. While it believes the tapes were destroyed, the bank didn’t get proof of the destruction. As a result, the bank was ordered to improve its security practices and warned that fines would be next if full compliance was not met.

Perhaps most impactful are regulations like Europe’s GDPR. Under these rules, multinational corporations are being scrutinized more than ever before for their management of digital data.

Inspired by GDPR, many similar new regulations are being put into place here in the US. If you’re not up-to-date on the changing laws, you could make a costly mistake. ITAD providers know the laws and make sure they’re always in compliance. It’s less hassle for you and makes sure your data destruction project is done correctly.

Make sure you partner with a responsible and certified ITAD provider. Look for certifications from NAID AAA, R2, e-Stewards, and ISO 9001. These four are only given to e-recyclers who pass surprise audits to guarantee they follow laws, use environmentally responsible practices, and maintain security at all stages of data destruction.

John Shegerian is the co-founder and executive chairman of ERI, the largest fully integrated IT and electronics asset disposition provider and cybersecurity-focused hardware destruction company in the United States. Learn more at eridirect.com.