BRANDED CONTENT

MARCH 25, 2024

CYBERSECURITY & DATA PROTECTION

With the Internet of Things on a perpetual increase, hundreds of thousands of employees working from home, and devices containing sensitive data leaving offices and entering homes as a commonplace occurrence, data security concerns have exponentially increased compared to less than a decade ago.

Corporate cybersecurity breaches have become more frequent, and with threats and fines mounting as we become increasingly reliant on cloud-based computing and other online innovations, cybersecurity has become more important than ever.

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

This special supplement to the Los Angeles 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.

CYBERSECURITY & DATA PROTECTION

Enhancing Business Resilience Against Cyber Threats

By KEVIN TADEVOSYAN

KEVIN TADEVOSYAN
CEO, CYBERDUO
KT@CYBERDUO.COM
CYBERDUO.COM

In an era where the digital landscape is continuously evolving, protecting your business from cyber threats has never been more crucial. As digital transformation accelerates, so does the sophistication of cybercriminals, making cybersecurity a critical concern for organizations seeking to protect their assets, data and reputation. CyberDuo, with over a decade of experience in the cybersecurity field, stands at the forefront of researching and implementing advanced defensive strategies. This expertise forms the basis of our recommendations for businesses aiming to bolster their cyber defenses effectively.

The cyber threat landscape is diverse, encompassing ransomware, phishing, data breaches and more. These threats can disrupt operations, incur significant financial losses, and damage business reputations. However, through rigorous security practices and informed strategy, organizations can significantly mitigate these risks. Below are research-backed strategies and best practices for enhancing cybersecurity posture.

ROBUST PASSWORD MANAGEMENT AND AUTHENTICATION PROTOCOLS

Weak passwords continue to be a critical vulnerability in security architectures. Research underscores the necessity of complex, unique passwords alongside the implementation of multi-factor authentication (MFA) as fundamental barriers against unauthorized access. MFA, in particular, has been identified as a significant deterrent, complicating attackers' efforts to exploit compromised credentials.

SYSTEMATIC SOFTWARE MAINTENANCE

The exploitation of software vulnerabilities is a common attack vector. A disciplined approach to software updates and patch management is essential for closing security gaps. Studies have shown that regular patching can prevent many cyber attacks, as these often leverage known vulnerabilities that have not been addressed by users.

CYBERSECURITY AWARENESS AND TRAINING

Human error is frequently a contributing factor in successful cyber attacks. The value of comprehensive cybersecurity training cannot be overstated, equipping employees with the knowledge to recognize and avoid potential threats. Ongoing education on evolving cyber threats and safe online practices is crucial in creating a culture of cybersecurity awareness within organizations.

NETWORK SECURITY ENHANCEMENTS

Protecting the integrity of network infrastructures is paramount. This involves deploying firewalls, employing encryption standards for data in transit and securing wireless access points. The segmentation of networks can also limit the spread of cyber threats internally, protecting sensitive data and systems from widespread compromise.

PRUDENT ACCESS CONTROL MEASURES

Access control is a critical aspect of cybersecurity, ensuring that only authorized individuals have access to specific data and systems. Applying the principle of least privilege, where users are granted the minimum level of access necessary for their role, reduces the risk of internal and external breaches. Regular audits of access rights and permissions are recommended to ensure that access controls remain aligned with organizational needs and security policies.

DATA BACKUP AND RECOVERY PLANS

The importance of reliable data backup and recovery procedures has been highlighted by the increasing frequency of ransomware attacks. Regular, secure backups of critical data can significantly reduce the impact of such attacks, facilitating quicker recovery and minimizing operational downtime. Backup strategies should include off-site or cloud storage solutions to ensure data availability in the event of a physical disaster or cyber incident.

INCIDENT RESPONSE PREPAREDNESS

Despite robust preventive measures, the potential for a security breach remains. An effective incident response plan is essential for quickly identifying, containing and mitigating attacks. Such plans should be regularly reviewed and updated in line with evolving cyber threats and organizational changes. Simulated cyber attack exercises can also be invaluable in testing the effectiveness of response strategies and identifying areas for improvement.

Cybersecurity is a dynamic field, requiring constant vigilance and adaptation to new threats. Through a combination of technical controls, informed policies and a culture of security awareness, businesses can significantly enhance their resilience against cyber threats. As the digital landscape continues to evolve, so too must the strategies we employ to protect it.

Kevin Tadevosyan is president and CEO of CyberDuo. To learn more, visit CyberDuo.com.

CYBERDUO

CYBERDUO

Los Angeles based Managed IT and Cybersecurity Services Provider

Since 2014, CyberDuo has been at the forefront of addressing IT and Cybersecurity challenges for businesses based in Los Angeles. As a local company deeply embedded in the community, we pride ourselves on delivering personalized, cutting-edge solutions that protect and empower local businesses.

Managed IT Services
Cybersecurity
IT Strategy and Consulting
Cloud and Cloud Security

ask@cyberduo.com
cyberduo.com
855-933-6638

CYBERSECURITY & DATA PROTECTION

Why Responsible E-Waste Data Destruction is Critical for Businesses

Electronics must enter the circular economy

By JOHN SHEGERIAN

When you have an electronic item that's no longer needed or is broken and doesn't work, it becomes e-waste. At that point, they may be refurbished, repurposed, or recycled. The 2020 Global E-Waste Monitor reported that 59.1 million tons of e-waste was generated in the world. That was an increase of 21% from 2015. The report estimated that the rate will reach 81.6 million tons by 2030. It's a mind-blowing amount of unused or broken electronics.

Smartphones, tablets and computers are some of the common types of e-waste, and most contain rechargeable lithium-ion batteries. They need to be carefully recycled, starting with data destruction. If your business is giving away or selling old electronics to save time and money, there are legal and ethical implications you're overlooking.

Businesses have an ethical responsibility to operate in a way that protects customer data. If you're processing credit cards, in possession of medical information or PII like an SSN or tax ID number, or keeping dates of birth, addresses, and phone numbers, it's your responsibility to keep it secure and wipe that information from hard drives when an electronic device is no longer being used.

Plus, businesses need to promote environmental responsibility, which is also part of proper e-waste disposal. You cannot just toss your company's older tablets and phones into the trash. E-waste harms the environment by leaching heavy metals into the soil and water. While today's landfills are lined, there's no guarantee that those liners will still be intact 100 years from now, and it can take plastic, glass and other components longer than that to decompose.

If you hire a company to take them away without thoroughly vetting that company, they could be saving money and shipping things to other countries for processing. The problem is other countries may use child labor or incinerate items without filtration, which releases toxins into the air.

Consumers have a lot of laws protecting them from harm when it comes to the information that's collected about them. The Privacy Act of 1974 requires agencies to follow "Fair Information Practices" when gathering and handling personal information. Agencies are also restricted on how they can share that information with others. If a person's right to privacy is violated, they are entitled to sue.

There's also the Right to Financial Privacy Act of 1978 that specifies these protections for banks and other financial agencies. Banks, government agencies and others must keep your personal information hidden and do everything possible to protect your PII. Since then, there have been several others.

One of the biggest laws today when it comes to data destruction is the Health Insurance Portability and Accountability Act of 1996. It requires health information to be kept private. Personally identifiable health information (PHI) must be protected at all times – past, present and future. Healthcare providers, health plans and healthcare clearinghouses have to ensure data of any PHI is destroyed or kept secure to avoid theft.

To add to this, 2009's Health Information Technology for Clinical and Economic Health Act mandates that any data breaches are reported to both the US Department of Health and Human Services and affected patients.

The Gramm-Leach-Bliley Act of 1999 is another biggie. Anything like a bank balance, account numbers and other private banking information is protected by this law. Banks, brokerages, insurance companies and credit unions must keep your banking information private and secure.

WHAT ARE THE BEST PRACTICES FOR E-WASTE DISPOSAL?

When you have any electronics that are no longer needed, you need to ensure that data wiping or physical destruction takes place. Data wiping is done using one of several methods.

- **Degaussing –** High-powered magnetics wipe information from magnetic devices like magnetic tapes, floppy disks and older hard disk drives.
- **Overwriting –** Special software is used to rewrite nonsensical patterns of binary code over older material until it's been rewritten so much that it's impossible to get back to older information.
- **Reformatting –** You can restore a device to factory settings, but that's not good enough for devices with PII. It may remove connections to old ones, but the information is still buried deep within and can be accessed by someone with the proper knowledge.

If a device has no life left, shredding it into tiny pieces and recycling the glass, plastic and metals is better. But, once you've done this, the item is no longer usable. For electronics that still have life left, overwriting or degaussing are often used before the items are refurbished for resale.

You want to make sure the company you partner with is certified by R2, NAID, SOC 2 and e-Stewards.

John Shegerian is the Chairman/CEO of ERI, the largest cybersecurity-focused hardware destruction and electronic waste recycling company in the United States. Learn more at eridirect.com.

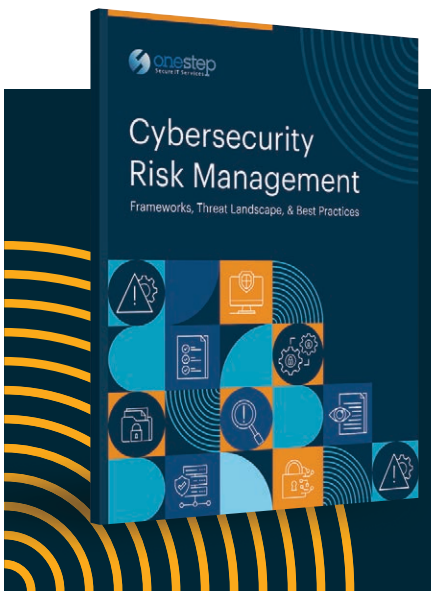
ONE STEP
SECURE IT
Complete IT & Cybersecurity Protection for Your Business

We are an outsourced IT company with over three decades protecting our customer's data from breaches to alleviate the dread of cyber attacks, costly downtime, and loss of customer trust.

Achieve peace of mind and separate yourself from the competition with our holistic approach to managing your network.

Our expertise includes Cybersecurity, Managed and Co-Managed IT, Information Security, and Compliance Services.

Keep your business secure. Contact us to talk to an IT and security expert at **(623) 227-1997** or visit us at **www.OneStepSecureIT.com/contact**



Begin Strengthening Your Business' Defenses

with our Free Comprehensive eBook on Cybersecurity Risk Management—tailored for business leaders seeking to safeguard their companies from downtime and expensive data breaches.

Scan to download or visit:
www.OneStepSecureIT.com/crm-ebook

onestep
Secure IT Services

CYBERSECURITY & DATA PROTECTION

Audit Committees Prioritize Cybersecurity, Enterprise Risk Management in New Survey

Two-thirds of audit committee members see opportunities to improve effectiveness

The recent "Audit Committee Practices Report: Common Threads Across Audit Committees," a joint effort between Deloitte's Center for Board Effectiveness and the Center for Audit Quality (CAQ), identified cybersecurity as the top priority in the next 12 months.

A total of 266 respondents participated in this year's survey, most of whom are from US public companies (74%), and of which 81% have more than $700 million in market cap.

Respondents cited enterprise risk management (ERM) as the No. 2 priority, demonstrating a broader, more holistic view of risk. Meanwhile, trending topics like artificial intelligence (AI) governance and environmental, social and governance (ESG) reporting are receiving comparably less attention.

"We are seeing the role of the audit committee continue to evolve and adapt as demands on oversight responsibilities change with the business environment and investor expectations," said Vanessa Teitelbaum, senior director, Professional Practice at CAQ. "Audit committees are zeroed in on one of their core responsibilities: overseeing enterprise risk programs at large. While their agenda continues to grow and expand, key areas like cybersecurity and ERM remain a central focus."

In addition to cybersecurity and ERM, finance and internal audit talent (a new entry in this year's survey), compliance with laws and regulations, and finance transformation rounded out the top five priorities. Although the majority of respondents view internal audit as an effective function — one that adds demonstrable value — nearly 80% believe there is an opportunity for internal audit to add even more value. Audit committees are also increasingly prioritizing compliance with laws and regulations, with more than one-third citing it as a top-three priority, a significant increase from last year.

CYBERSECURITY REMAINS NO. 1 PRIORITY FOR AUDIT COMMITTEES, FOLLOWED BY ERM

Cybersecurity topped the list of committee priorities by nearly 20 percentage points over ERM. Notably, 58% of respondents said the audit committee has primary oversight over cybersecurity, with 25% indicating the full board has oversight responsibility. Sixty-nine percent of respondents highlighted cybersecurity as a top concern in the next 12 months, with three in ten ranking it No. 1.

The heightened focus on cybersecurity is likely due to greater disclosure requirements from regulatory agencies. The US Securities and Exchange Commission (SEC), for example, is requiring new disclosures on cybersecurity risks and incidents, as well as management and strategy, including an explanation of oversight processes.

When considering what additional expertise would enhance the audit committee's effectiveness, cybersecurity was highlighted as the top area (44%). This is particularly notable given that almost half (48%) of respondents said they have some level of cybersecurity expertise on the committee.

The evolving risk landscape and emerging risks have put an increased spotlight on ERM. Nearly half of respondents indicated that ERM will be a top focus area in the next 12 months. More than three quarters (85%) of respondents reported some level of ERM expertise on the audit committee, positioning it to effectively oversee management's risk programs.

Learn more at deloitte.com.

YOUR CAREER AWAITS

Come join our media sales team if you are looking to:

- Represent award-winning business publications
- Consult with C-level executives
- Network at our exclusive events
- Earn unlimited commission potential
- Receive a great benefits package

Only highly motivated, dynamic, and creative advertising sales account managers need to apply.
Send your resume to kgarcia@labusinessjournal.com

LOS ANGELES BUSINESS JOURNAL