STRATEGIC GUIDANCE

LMG SECURITY

TOP CYBERSECURITY CONTROLS OF 2023

At LMG, security experts constantly monitor the latest threats, track data breach trends, analyze cyber regulations and legal cases, and evaluate the effectiveness of controls and solutions.

Based on this extensive and continuous research, our experts have identified the top cybersecurity controls for today's risks. These controls have been selected because they are specifically relevant due to today's changes in the threat landscape, cybersecurity solutions space, and/or regulatory environment. This timely and prioritized list is designed to augment a comprehensive list of controls such as the NIST Cybersecurity Framework or ISO 27001.

When selecting the top controls, LMG's analysts consider:

- The effectiveness of each control against current threats and vulnerabilities.
- The relative financial investment and resources required in order to implement the control.
- The importance of the control for demonstrating compliance or meeting third-party expectations.

And now, without further ado...

THE TOP SECURITY CONTROLS OF 2023

1. Advanced Multifactor Authentication (MFA)
2. Extended Detection and Response (XDR)
3. On-Demand Cybersecurity Awareness Training
4. Identity and Access Management (IAM)
5. Effective Patch Management
6. Attack Surface Monitoring
7. Cloud Configuration Management
8. Continuous Security Monitoring
9. Incident Response Testing and Training
10. Next-Generation Backups
11. Data Discovery & Mapping
12. Qualified Security Leadership

1 Advanced Multifactor Authentication (MFA)

Multifactor Authentication (MFA) is a must for all Internet-facing systems, and it is increasingly deployed throughout internal infrastructures as well. Use strong authentication technologies, such as hardware tokens or smartphone apps, and move away from weaker MFA tools such as SMS (text messages), phone calls, emailed codes, and more. The U.S. government recommends using "phishing-resistant" MFA technologies to foil social engineering tactics.

Configuration matters – with the rash of "MFA Fatigue" attacks, defenders need to limit the number of MFA attempts and leverage more advanced options like Microsoft's number matching. Consider deploying adaptive MFA technologies that use context such as location, device type, and time to automatically provide appropriate MFA challenges. Read this MFA Tip Sheet for more information and best practices.

These controls have been selected because they are specifically relevant due to today's changes in the threat landscape, cybersecurity solutions space, and/or regulatory environment.

2 Extended Detection and Response (XDR)

Endpoint Detection and Response (EDR) technology quickly detects and neutralizes threats and facilitates effective response. Simple EDR is not enough these days: organizations need to leverage similar techniques holistically across the network, cloud, and endpoints of all kinds. Enter Extended Detection and Response (XDR), which centralizes and streamlines security visibility, detection, and response. XDR reduces risk, simplifies operations, and decreases the total average cost of a data breach by $190,622, according to IBM.

3 On-Demand Cybersecurity Awareness Training

Humans are a critical part of your security arsenal. Every organization needs to keep security top-of-mind with a robust training program. Gone are the days when an annual webinar would suffice. Today, cybersecurity training needs to be provided monthly or more frequently to effectively address the latest threats. Consider on-demand cybersecurity awareness training with short videos and quizzes to train and test your team. Curate the content appropriately to ensure it addresses your organization's risks.

4 Identity and Access Management

Hackers have perfected the art of account takeover, leveraging user, administrator, and system accounts at every stage of the attack. What's more, cybercriminals offer insiders lucrative payments to help hack their employers. Modern Identity and Access Management (IAM) systems centralize identity management throughout an enterprise, facilitating quick onboarding and offboarding, effective role-based access and restrictions, detection of suspicious activity, and more. Every organization should have an IAM system and regularly maintain it to minimize the risk of account takeovers and insider attacks.

5 Effective Patch Management

Software exploitation was the top initial infection vector in 2021, according to Mandiant. Today's hackers can easily shop for exploits on the dark web and develop new exploits using stolen source code and bug reports. All organizations need effective patch management tools and processes, including operating systems and third-party applications. This includes automated deployment whenever possible, as well as strong patch verification systems and alerts when errors occur. With the rise of zero-day software vulnerabilities, defenders need to plan their response and be ready to deploy critical patches after hours and on weekends when needed.

6 Cloud Configuration Management

As data moves to the cloud, security responsibility moves with it. Make sure to conduct a cloud application security review upon migration, and plan for ongoing configuration maintenance. This includes common platforms such as Microsoft 365, AWS, and others. Ensure that your configuration review is conducted by trained and experienced personnel or outsource as needed. Unfortunately, many organizations overlook cloud application security and suffer needless data breaches as a result of minor configuration errors.

7 Attack Surface Monitoring

Attackers are relentless—and defenders need to continuously monitor their attack surface to prevent security breaches. Typically, this requires continuous vulnerability scanning, configuration checks, and automated asset discovery. In today's threat landscape, monthly vulnerability scans are no longer sufficient. Defenders must employ automated tools to scan daily or even hourly and alert a ready response team when weaknesses are detected.

8 Continuous Security Monitoring

Every organization needs 24/7 monitoring. Attackers frequently launch attacks after normal business hours, or on holidays and weekends, when organizations have fewer staff to monitor and respond to alerts. Outsourced monitoring is critical for achieving effective 24/7 coverage, unless your organization is large enough to maintain a trained and qualified internal monitoring and response team.

9 Incident Response Testing and Training

Organizations that formally establish their incident response (IR) team and regularly test their IR plans save $2.66 million on the average cost of a data breach, according to IBM. Assign incident response roles, document policies and procedures, and conduct tabletop exercises to train your staff and identify gaps in your response.

10 Next-Generation Backups

Attackers deploy sophisticated tools to extract passwords and valuable data from backup files, and routinely work to destroy backups. All organizations should configure immutable backups, which block even administrators from modifying or deleting data. Prevent attackers from accessing backup files and the backup environment using multilayer security. To accomplish this, invest in modern backup tools that support immutability, as well as trained and experienced professionals to configure and test your systems.

11 Data Discovery & Mapping

The quickest and most effective way to reduce cybersecurity risk is to delete unnecessary data—but most organizations do not maintain a comprehensive data inventory, and therefore cannot properly address risk and align security investments. All too often, data inventories are conducted in an emergency, post-breach, resulting in exorbitant bills. Proactively conduct data discovery and data mapping using automated tools with robust reporting features.

12 Qualified Security Leadership

Every organization needs an experienced CISO or security leader to provide effective guidance and meet compliance requirements. Regulators such as the FTC and NYDFS now require that certain organizations hire a "qualified individual" to oversee their cybersecurity programs. IBM found that having a skilled CISO decreased the average cost of a breach by $144,914. However, skilled security leaders are hard to find and expensive to hire. Small to midsized organizations can save money and gain access to skilled leadership with a fractional CISO.

For more information or help implementing the Top Cybersecurity Controls, contact LMG's team of experts.

Cybersecurity evolves rapidly—both adversary tactics and defensive solutions. Tune in regularly for the latest updates to LMG's Top Security Controls.

LMG™ SECURITY

info@LMGsecurity.com
855-LMG-8855

LAST REVISED 2022-12-22

www.LMGsecurity.com