the NetWork

LeadingIT

Chicagoland CybersecurITy Support

December 2023

- Cost-Effective Cybersecurity: How CFOs Can Leverage Managed Services for Savings
- Cloudy with a Chance of Cyberattacks: Protecting Your Cloud Resources
- 7 Mitigation Strategies For Protecting Against Insider Threats
- Cyber Safety On Four Wheels: Protecting Your Connected Car From Threats
- Gaming for Good: LeadingIT Joins Extra Life to Change Kids' Health

GoLeadingIT.com 815-893-2525 @goleadingit

Cost-Effective Cybersecurity

How CFOs Can Leverage Managed Services for Savings

In the intricate web of today's digital world, where every click and keystroke can have profound consequences, ensuring the safety of sensitive data isn't just an IT challenge—it's a financial imperative. Chief Financial Officers (CFOs) are seeking innovative ways to balance robust security measures with cost-effectiveness. One such solution gaining traction is leveraging managed services. This strategic approach not only fortifies a company's defense against cyber threats but also offers substantial cost savings.

Understanding the Real Cost of Cybersecurity

Cybersecurity incidents can wreak havoc on a company's financial stability. The costs associated with data breaches, system downtime, and regulatory fines are substantial. In 2023, the global average cost of a data breach reached 4.45 million USD, marking a 15% increase over three years, as reported by IBM.

Behind the statistics and news headlines are real stories of financial loss, legal battles, and shattered trust. The aftermath of a cyber incident isn't just about monetary damages; it's about rebuilding shattered confidence, both internally and among customers. CFOs recognize that the financial impact of cybersecurity isn't merely a balance sheet concern; it affects the heart of the organization.

The Benefits of Managed Services

In this challenging landscape, CFOs are turning to a beacon of hope: managed services. Imagine having a dedicated team of experts watching over your digital realm, proactively defending against threats.

These services offer a wide range of support, from real-time threat monitoring to swift incident responses, vulnerability assessments, and compliance management. By entrusting these responsibilities to specialists, companies gain access to a talented pool of professionals without the burdensome costs of maintaining an in-house security team. Managed services ensure that a company's online defenses are not only current but also flexible, adapting to the ever-evolving threat landscape.

In regard to pricing, managed services operate on a subscription-based model, offering predictable monthly costs. This predictability is a game-changer for CFOs, allowing them to allocate budgets with confidence, free from the uncertainties that often come with managing cybersecurity internally.

Additionally, these services are designed to be flexible, scaling up or down based on the organization's specific needs. This adaptability ensures that resources are used optimally, eliminating unnecessary expenses while maintaining top-notch security.

Continue reading on page 7

Pictured on the cover: Keegan, Scott, Salvador, Laura, Daniel, Kyle

Cloudy with a Chance of Cyberattacks: Protecting Your Cloud Resources

In 2022, cloud users were hit hard by security issues, including data breaches and intrusions, with a staggering 80% of organizations facing serious cloud security incidents. What's even more concerning is that 25% fear they might have experienced a cloud breach without knowing it.

Cloud computing has become an indispensable part of businesses and individuals alike. But as more and more sensitive data migrates to the cloud, it becomes imperative to understand cloud vulnerabilities, implement security best practices, and establish a robust incident response plan. Keep reading to learn more.

Understanding Cloud Vulnerabilities

Cloud vulnerabilities stem from various sources. Data breaches can occur if proper safety measures are overlooked, allowing unauthorized access to sensitive information. Misconfigurations and phishing schemes create entry points for cybercriminals, exploiting deceptive tactics to infiltrate cloud accounts. Additionally, internal threats, whether intentional or accidental, pose significant risks. Recognizing and addressing these vulnerabilities are essential steps toward enhancing cloud security and safeguarding valuable data in the ever-changing digital landscape.

To protect against an increasing array of cyberattacks now targeting cloud services worldwide it is essential for organizations to put comprehensive security strategies in place addressing each risk accordingly.

Security Best Practices:

Implementing security best practices is the first line of defense against cloud-based cyberattacks. Here are a few to keep in mind:

• Keep Your Data Safe: Make sure your data is protected by encrypting it to stop anyone from accessing it without permission.

• Extra Verification: Add an extra layer of security by using Multi-Factor Authentication.

• Control Who Accesses What: Limit who can access what in your system. Only give users the minimum access they need.

• Stay Updated: Always update your software to the latest version. These updates often include patches that fix known security issues.

• Guard Your Network: Use firewalls and detection systems to keep an eye on your network.

• Knowledge is Power: Educate your employees about potential threats like phishing. When they know what to look out for, they can help keep your system safe.

Continue reading on page 7

Gaming for Good: *LeadingIT Joins Extra Life to Change Kids' Health*

The LeadingIT team recently participated in the Extra Life charity gaming event, an initiative uniting gamers to support children's health through Extra Life. Since 2008, Extra Life has raised over $100 million for Children's Miracle Network Hospitals. Our team gathered in office and remotely to playing games on any platform and seek sponsorship from friends and family to make a difference in children's lives. Our staff's enthusiastic participation reflects our commitment to this cause, and together, we can play games, change kids' health, and help create a brighter future for those in need.

extra life™
Play Games. Heal Kids.

BENEFITING
Children's Miracle Network Hospitals®

Pictured above: Kyle and Daniel

Cyber Safety On Four Wheels:
Protecting Your Connected Car From Threats

The world is increasingly connected through the Internet of Things (IoT), and the automotive industry is no exception. According to Deloitte, there will be over 470 million internet-connected cars in use by 2025.

These high-tech vehicles offer drivers a host of convenient features, including vehicle-to-vehicle (V2V) communications, remote parking, and sophisticated infotainment systems. However, with these benefits come certain risks, as malicious actors seek to exploit vulnerabilities in these vehicles. Let's explore how to protect your connected car from cyber threats and ensure the safety of your digital ride.

Ways Connected Cars Can Get Hacked

Internet-connected cars continuously transmit and receive data from various sources. In fact, they are equipped with hundreds of sensors that transmit data to connected computers. While this data enhances the driving experience, it also presents opportunities for cyber-attacks. Here are a few ways your car can be vulnerable to hacking:

1. Physical Access: Attackers can physically break into connected cars and access their Electronic Control Unit (ECU) systems. Once inside, they can manipulate and take control of the vehicle's functions.

2. Software Vulnerabilities: Malicious actors can find vulnerabilities in the ECU and install malicious code, compromising the car's security and potentially putting the drivers and passengers at risk.

How to Secure Your Connected Car

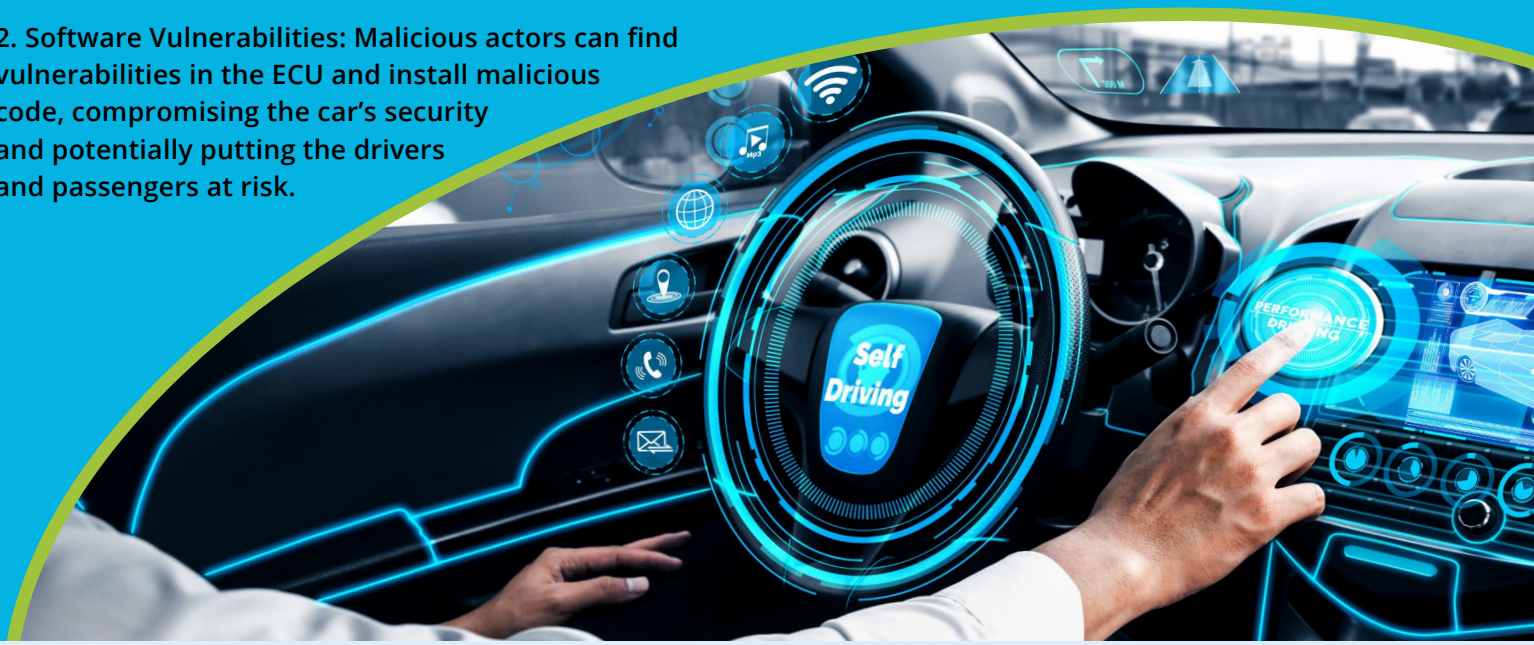
Protecting your connected car from cyber threats requires vigilance and careful practices. Here are some key steps to ensure your car's safety:

1. Remove Dongles: Be cautious of any aftermarket devices or dongles (devices that monitor performance and location) that connect to your car's OBD-II port. Some of these devices may pose security risks. If you don't need them, remove them.

2. Key Fob Safety: Store your car's key fob in a secure place, ideally in a metal drawer or Faraday bag. This prevents attackers from intercepting the fob's signal and unlocking or starting your car remotely.

3. Regular Software Updates: Ensure that your car's software is regularly updated. Manufacturers often release updates that patch security vulnerabilities and enhance protection.

Connected cars can offer incredible convenience and innovation, but it's essential to prioritize cybersecurity. As automotive technology continues to expand, it's crucial to stay informed about the latest developments and security measures. By following the steps outlined in this article and remaining vigilant, you can enjoy the benefits of your connected car while simultaneously minimizing the risks associated with cyber threats.



7

Mitigation Strategies For Protecting Against Insider Threats

Defending against insider threats requires a holistic strategy integrating technology, policies, and employee awareness. Here are a few strategies to incorporate:

1

Access Control and Monitoring: Limit employee privileges to essential tasks and use real-time behavior analytics to detect anomalies.

2

Employee Training: Cultivate a security-conscious culture through regular employee training. Educate them on recognizing phishing attempts and securing passwords, making them the first line of defense.

3

Data Encryption and DLP Solutions: Encrypt sensitive data both at rest and in transit. Utilize Data Loss Prevention solutions to monitor and block unauthorized data transfers, ensuring information is protected throughout its journey.

Continue reading on page 8

Cost-Effective Cybersecurity continued from pg 2...

Measuring ROI

One of the challenges faced by CFOs is quantifying the return on investment (ROI) in cybersecurity expenditures. Managed services provide a clear advantage in this regard. The ROI of managed services can be gauged in terms of reduced incident response times, minimized system downtime, and lower recovery costs in the event of a breach.

Furthermore, measuring the value of managed services goes beyond dollars and cents. With managed services comes enhanced customer trust and a fortified brand image, adding substantial value to the investment.

Managed services also contribute to operational efficiency, empowering internal teams to focus on what truly matters – fostering innovation, nurturing client relationships, and enhancing overall business performance. These benefits directly impact the bottom line, offering a tangible measure of the ROI on cybersecurity investments.

Conclusion: Fiscal Diligence Meets Robust Cybersecurity

CFOs play a pivotal role in safeguarding an organization's financial health, and cybersecurity is a significant aspect of this responsibility. By embracing managed services, CFOs can ensure robust cybersecurity measures while optimizing costs. The predictable expenses, scalability, and measurable ROI make managed services an attractive option for CFOs seeking a cost-effective and efficient cybersecurity solution.

Cloudy with a Chance of Cyber Attacks continued from pg 3

• Backup Your Data: Regularly back up your data to a secure location. This way, even if there's a security problem, your important information is safe.

• Follow the Rules: Compliance with data protection laws and industry standards ensures you're meeting the necessary security standards.

• Use Your Provider's Tools: Take advantage of the security tools your cloud service provider offers.

• API Safety: If your apps use APIs, make sure they're secure to prevent attacks from sneaky code.

• Check Your Partners: If you work with outside vendors, make sure they're as committed to safety as you are.

• Stay Alert: Implement continuous monitoring of your cloud space. This way, if there's anything suspicious, you can catch it and respond quickly.

Incident Response

No security system is perfect, so having a clear plan for when things go wrong is crucial. You need to know exactly what to do in case of an emergency. This plan involves quickly understanding the problem, containing it, getting rid of the threat, recovering any lost information, and learning from the experience to do better next time.

Practicing the plan makes perfect. By simulating different situations, you can figure out what works best and how to respond faster. But it's not just about the technical side – communication is key. Keeping everyone in the loop – stakeholders, employees, customers, and even regulatory authorities – helps maintain trust and ensures everyone knows what's happening and what their role is.

Conclusion: Preparation is Key To Navigating the Storm

The convenience, scalability, and flexibility offered by cloud services are unmatched, but we have to acknowledge the storm on the horizon: the constant threat of cyberattacks. Understanding vulnerabilities, adhering to security practices, and implementing a robust response plan are critical. With the right tools and proactive approach, organizations can safeguard their operations and data in the face of cyber storms.

7 Mitigation Strategies from pg 6...

4

Incident Response Plan: Develop a robust plan for insider threat incidents. Having clear procedures for investigation, containment, and recovery ensures a swift and organized response.

5

Background Checks: Thoroughly vet employees, especially those handling sensitive information. Regular updates on these checks are like periodic health check-ups, ensuring employees remain trustworthy over time.

6

Secure Third-party Relationships: Hold external partners to the same security standards as internal staff.

7

Continuous Monitoring: Insider threats evolve, so should your defenses. Regularly assess and update security policies and technologies.

Continue reading on our blog at goleadingit.com/blog

LeadingIT

Serving the Chicagoland area with offices in Woodstock, Downtown Chicago, and now in Manteno, IL.

LeadingIT

$1000 REFERRAL PROGRAM

WE LOVE REFERRALS!

Do you know an organization that needs fast + friendly IT and cybersecurity support?

If they sign up, you'll receive $1000!

LEARN MORE

GOLEADINGIT.COM/REFER

815-788-6041

WE ARE CELEBRATING!

Birthdays

Jaclyn Murray - December 8th

Christa Gibbons - December 14th

Anniversaries

George Huebner - 12/2/2022

George Howes III - 12/2/2022

Joel DeBoer - 12/2/2022