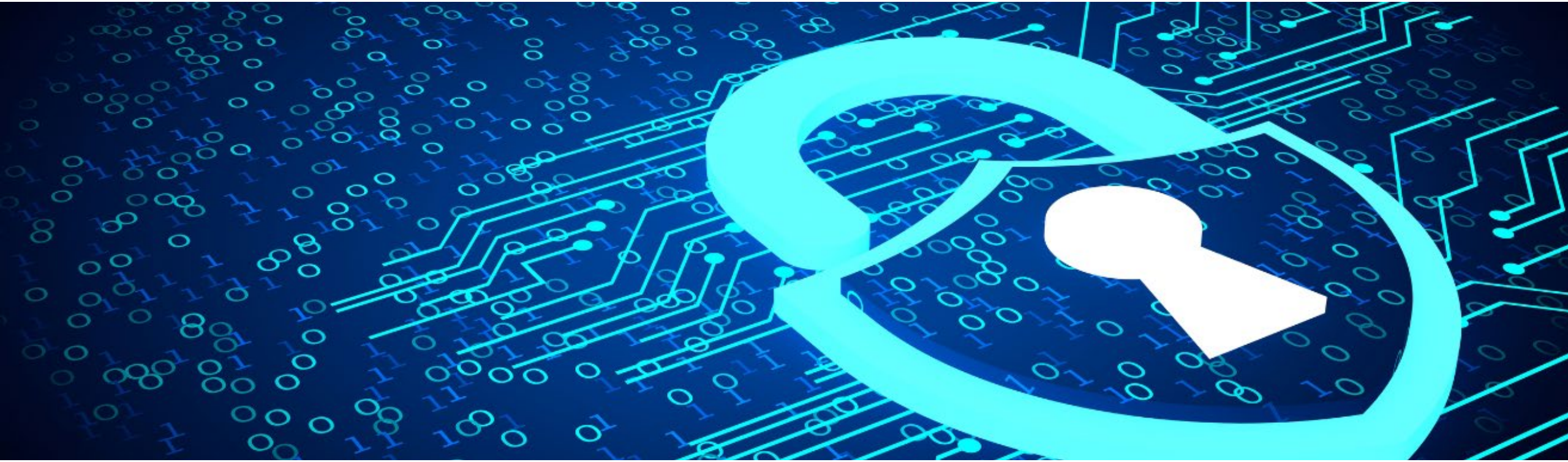


YOU'VE BEEN BREACHED; WHAT'S NEXT?

Thursday, December 5, 2024

GNYADA Dealer Webinars are Sponsored by:

Joel Ackerman

Principal
CLA (CliftonLarsonAllen LLP)

Direct 516-202-8668
joel.ackerman@claconnect.com

CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.

DMV-DIRECT

REGISTRATION, TITLING, & BEYOND...
CALL 718.747.0400

GNYADA's vehicle registration and titling service, DMV-DIRECT, has been dealers go-to source for fast, convenient, & reliable DMV services.

DMV-DIRECT provides many DMV related services, including:

- Permanent Registration Issuance
- Duplicate Titles In 3 To 5 Days
- Out-of-State Registration & Title Processing for 42 States
- On-Site Connecticut Plates Issuance
- Dial-In Information Verification
- In-Transit Processing
- Duplicate Registrations
- Registration Renewals
- Title-Only Transactions
- Plate Surrenders
- Dealer Plate Renewals
- Rental Plate Renewals
- Repossessed Vehicles Processing
- MV-82 & Transmittal Forms Supplied
- Boat Registrations – Renewed and Duplicates
- Trailer Plates
- Commercial Plates

January Education and Training Classes

January 7

Service Advisors Guide to Selling Service and Repair

January 8

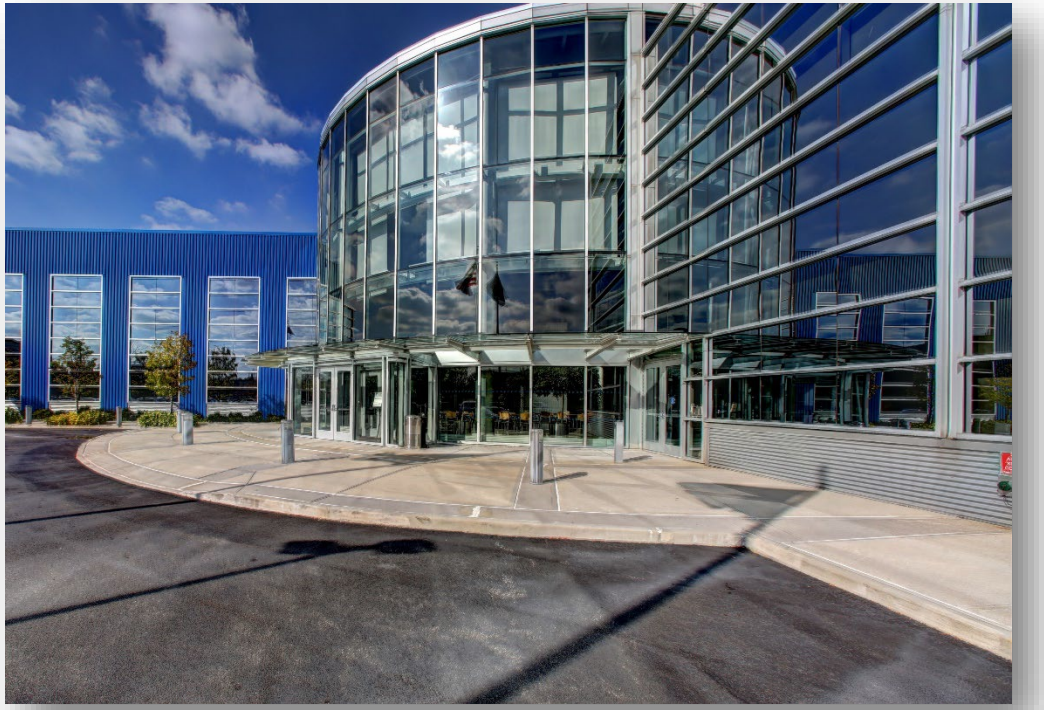
Mastering Negotiation in Sales

January 15

Notary Public Training & Test Prep

January 16

GNYADA Franchise Law Seminar



Visit www.gnyada.com/education to Register

onestep
Secure IT Services

RMF
RuskinMoscouFaltischek P.C.

YOU'VE BEEN BREACHED

WHAT'S NEXT?

IMPACT OF CYBER ATTACKS ON AUTO DEALERS

TODAY'S SPEAKERS

KEVIN MCADAM

Chief Revenue Officer at
One Step Secure IT

Over 25 years of experience in business technology. Specializes in optimizing and securing IT infrastructure for auto dealers.

ANDREW GARBARINO

Co-Chair of RMF's White Collar Crime and Investigations Law Practice

Represents corporations and professionals in high-stakes cases and advises on data breaches and internal investigations.

OVERVIEW

Our presentation today will cover five topics with a Q&A session at the end.

01 | Security Risks in Everyday Life

02 | Top 5 Cyber Threats

03 | The Auto Industry is a Target

04 | Consequences of a Breach

05 | Steps to Take After a Cyber Incident

06 | Q&A Session

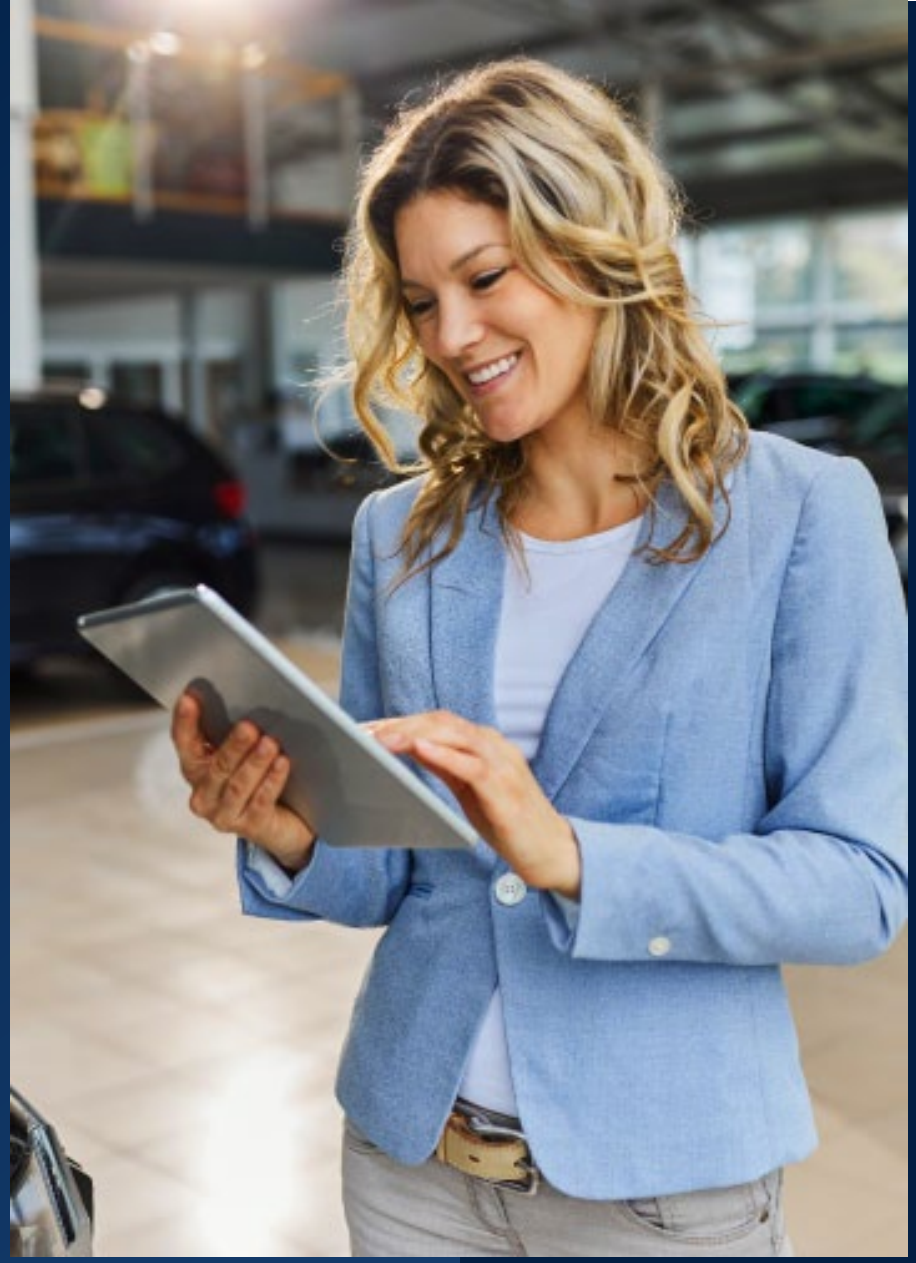
ONE STEP SECURE IT

Protecting your business from the threats you know, and the ones you don’t.

One Step Secure IT is 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.

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

Based in Phoenix, AZ, we proudly serve businesses nationwide.



RUSKIN MOSCOU FALTISCHEK

Smart Counsel. Straight Talk.

Founded in 1968, we are a Long Island law firm offering legal services across many areas.

Our Cybersecurity and Data Privacy Practice Group supports businesses, including auto dealerships, with cybersecurity, privacy, and data protection needs.

Services include data breach response, compliance with laws like HIPAA and GDPR, and drafting policies such as privacy agreements and incident response plans.

Our group also helps with board governance, executive coaching, and employee cybersecurity training, focusing on current challenges and future risks.

SECURITY RISKS OF TRAVELING ABROAD

Vacationing while traveling to London and Paris

Visiting the Great Wall of China

Stopping over in India, Egypt, and Israel

VULNERABILITIES WHEN UPGRADING EQUIPMENT

The internal IT team upgrades one of the desktops.

The old tower is left in an area where the maintenance staff picks it up, believing it’s meant for the dumpster.

An employee from the waste removal company brings it home.

SECURITY RISK OF ONLINE DATING

An employee meets a woman named Veronica online.

Over a period of days, they exchange a variety of photos, including clearly identifiable face shots.

Veronica threatens to publish the messages and photos on LinkedIn if she isn’t paid a BitCoin.

MEET VERONICA

DO YOU MAKE BETTER DECISIONS

IN A STATE OF PANIC OR WHEN WELL PREPARED?

TOP 5 CYBER THREATS

The threats all businesses should be aware of.

05 | Business Email Compromise

04 | Third-Party Exposures

03 | Human Error

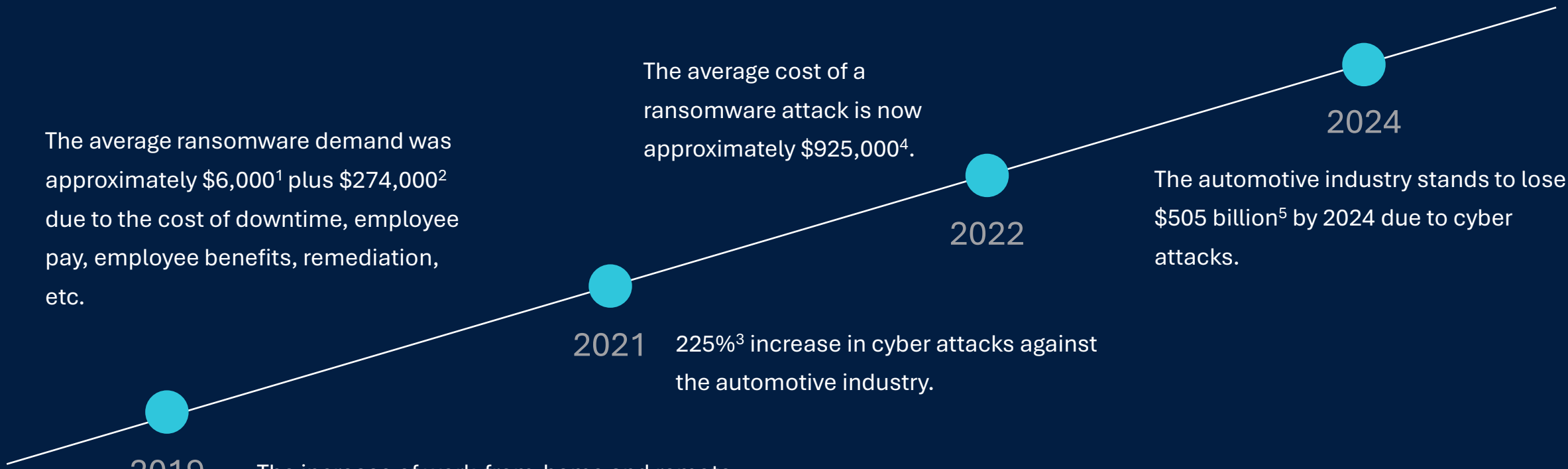
02 | Inside Wrongdoers

01 | Ransomware

THE AUTO INDUSTRY IS A
GROWING TARGET...

ON THE RISE

Ransomware has been on an uptick following the pandemic.



2019

The average ransomware demand was approximately $6,000[1] plus $274,000[2] due to the cost of downtime, employee pay, employee benefits, remediation, etc.

The increase of work-from-home and remote users opened new attack surfaces IT departments had not considered.

2021

225%[3] increase in cyber attacks against the automotive industry.

2022

The average cost of a ransomware attack is now approximately $925,000[4].

2024

The automotive industry stands to lose $505 billion[5] by 2024 due to cyber attacks.

Sources: 1. https://insider.govtech.com/california/the-true-cost-of-a-ransomware-attack 2. Sophos The State of Ransomware Report 2021. 3. https://scoop.market.us/automotive-cyber-security-statistics/ 4. Global Cyber Confidence Index 2023. 5. Forbes https://www.forbes.com/sites/stevetengler/2023/10/25/new-auto-cyber-study-reveals-threat-intelligence--or-lack-thereof/

IMPACT ON THE AUTO INDUSTRY

The last several years have been successful for many dealerships, drawing the attention of cyber criminals who see them as easier targets than larger businesses.

Dealerships experienced an average of 16 days of downtime after a ransomware attack.

Average ransomware payout of $228,125[1]

84%[1] of customers say they would not buy another vehicle from a dealership if a data breach compromised their information.

Sources: 1. https://securityintelligence.com/news/hackers-increasingly-targeting-auto-dealers/

THE TOP 5 CONSEQUENCES OF A DATA BREACH

05

Reputational Damage

04

Lawsuits & Investigations

03

Remediation

02

Barred from Working with Government

01

Organization No Longer Viable

DATA BREACHES

Top 5 things you may not know about them.

05 | 50 States=More Than 5 Statutes

04 | It’s Become Big Business

03 | Wall of Shame

02 | Costs

01 | Board & C-Suite Liability

18 U.S.C §1001

SO, YOU’VE BEEN BREACHED

HERE’S THE STEPS TO TAKE

01

Immediate Containment

Disconnect Affected Systems: Unplug compromised computers and servers from the network.

Preserve Evidence: Avoid turning off systems; document all actions taken.

01 Immediate Containment

Disconnect Affected Systems: Unplug compromised computers and servers from the network.

Preserve Evidence: Avoid turning off systems; document all actions taken.

02 Engage Incident Response Team

Notify IT Team: Alert your IT team or managed service provider.

Notify Insurance Carrier: If you have cyber insurance, contact the incident response hotline.

Contact Experts: Engage a law firm and cybersecurity professionals.

01 Immediate Containment

Disconnect Affected Systems: Unplug compromised computers and servers from the network.

Preserve Evidence: Avoid turning off systems; document all actions taken.

02 Engage Incident Response Team

Notify IT Team: Alert your IT team or managed service provider.

Notify Insurance Carrier: If you have cyber insurance, contact the incident response hotline.

Contact Experts: Engage a law firm and cybersecurity professionals.

03 Initial Assessment

Determine Scope: Identify affected systems and data.

Identify Attack Vector: Understand how the breach occurred.

04

Communication

Internal Notification: Inform senior management and relevant teams.

External Notification: Prepare communication for customers and stakeholders if necessary.

04 Communication

Internal Notification: Inform senior management and relevant teams.

External Notification: Prepare communication for customers and stakeholders if necessary.

05 Investigation

Collect Evidence: Secure logs and take system images.

Identify Malicious Activity: Look for indicators of compromise.

04 Communication

Internal Notification: Inform senior management and relevant teams.

External Notification: Prepare communication for customers and stakeholders if necessary.

05 Investigation

Collect Evidence: Secure logs and take system images.

Identify Malicious Activity: Look for indicators of compromise.

06 Eradication and Recovery

Remove Threats: Eliminate malware and close backdoors.

Patch Vulnerabilities: Apply necessary updates.

Restore Systems: Use clean backups to restore data.

07

Post-Incident Review

Analyze Incident: Conduct a post-mortem to understand the breach and response.

Update Policies: Revise security policies and response plans.

07 Post-Incident Review

Analyze Incident: Conduct a post-mortem to understand the breach and response.

Update Policies: Revise security policies and response plans.

08 Enhance Security Measures

Strengthen Controls: Implement firewalls, IDS, MFA, and encryption.

Employee Training: Conduct regular cybersecurity training.

07

Post-Incident Review

Analyze Incident: Conduct a post-mortem to understand the breach and response.

Update Policies: Revise security policies and response plans.

08

Enhance Security Measures

Strengthen Controls: Implement firewalls, IDS, MFA, and encryption.

Employee Training: Conduct regular cybersecurity training.

09

Continuous Monitoring

Monitor Systems: Implement ongoing monitoring for suspicious activity.

Regular Audits: Perform security audits and vulnerability assessments.

Q&A

DO YOU HAVE ANY QUESTIONS?

CONTACT US

KEVIN MCADAM

Chief Revenue Officer at
One Step Secure IT

623-227-1997

kmcadam@onesteptech.com

ANDREW GARBARINO

Co-Chair of RMF's White Collar Crime and Investigations Law Practice

516-663-6632

agarbarino@rmfpc.com

Take Advantage of Our FREE 27-Point Inspection

IS YOUR DEALERSHIP'S IT READY FOR PEAK PERFORMANCE?

Optimize your IT infrastructure for efficiency and security to prevent costly downtime and cyber threats.

Act now with a Free 30-minute consultation. We'll analyze your security practices and provide a custom report to strengthen your defenses.

Don't wait for a breach.
Proactively protect your business.
Get your free consultation today!

www.OneStepSecureIT.com/Gnyada-Webinar-27pt

UPCOMING

Staying on top of your cybersecurity is an ongoing process; we are here to simplify it. Stay in touch with One Step Secure IT...

Newsletter

One Step Secure IT company magazine, The Latest Byte is out next month.

Event

We will be attending the NADA Show: Jan. 24-26th. Say hello!

Booth #7651

Podcast

One Step Beyond Cyber Podcast Season 3 is releasing next year!