Cybersecurity Essentials – Building a Resilient Business in a Digital World

Daniel Silverman - Underwriting Director, Specialized CyberTech Risks, Global Specialty - The Hartford

Keith Tagliaferri - Director, Cyber Claim Practices - The Hartford

Andrew Correll - Senior Director, Cyber Insurability - SecurityScorecard

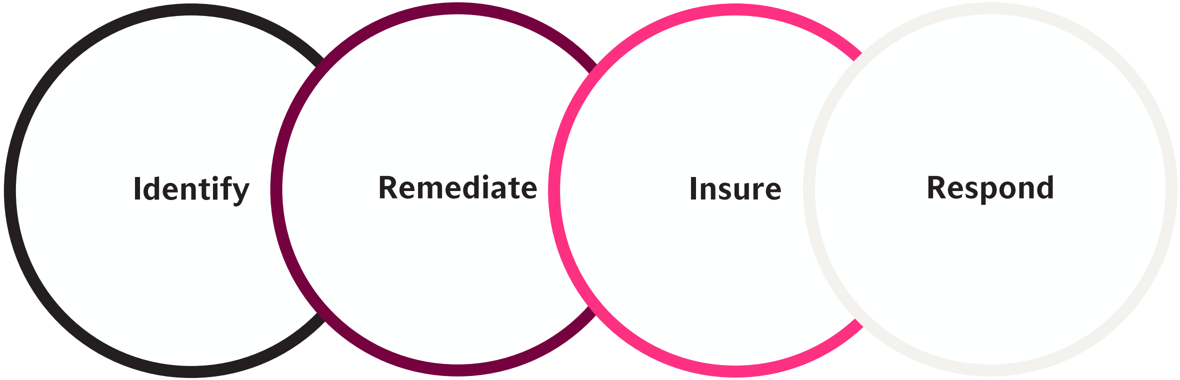
March 25, 2025

The Hartford: Cyber Underwriting and Risk Mitigation

The Hartford

Cyber Risk Management Eco-System

The Hartford Coverage & Cyber Services Portfolio



Cybersecurity Essentials:

Building a Resilient Business in a Digital World

Andrew Correll
Sr. Director,
Cyber Insurability

SecurityScorecard

What You’ll Learn Today

01 Understand the current cyber threat landscape for Small & Mid-Sized Businesses

02 Identify key areas of cyber risk

03 Learn practical steps to mitigate those risks

04 Discover resources to improve your cybersecurity posture

Understanding the Cyber Landscape for SMBs

The Increasing Cyber Threat to SMBs

- Cyber attacks are rapidly increasing, and Small and Medium-sized Businesses (SMBs) are frequently targeted.
- 43% of cyber attacks target small businesses.
- Business Email Compromise (BEC) is the #1 type of attack, and phishing is the #1 tactic.
- Small businesses are disproportionately hit due to fewer resources.

Common Types of Cyber Attacks

Ransomware

Encrypting data for extortion

Zero-Day Vulnerabilities

Unknown, unpatched software flaw being actively exploited

Business Email Compromise

Hijacking legitimate email systems for further access or to trick people into doing things

Real-World Impact

Ransomware

Colonial Pipeline suffered a ransomware attack in May 2021, halting fuel distribution and causing widespread disruption. They paid a $4.4 million ransom to regain access, but the pipeline was down for six days. The company incurred additional millions in remediation costs to restore full operations and security.

Business Email Compromise (BEC)

A Japanese company's US subsidiary lost $37 million in a 2019 BEC attack. Attackers compromised an employee's email, likely through phishing and spoofing. They then impersonated the employee to request fraudulent fund transfers. The company discovered the loss during a routine audit, demonstrating the severity of BEC attacks.

Key Areas of Cyber Risk for SMBs

Web Servers & Applications

Key Areas of Cyber Risk

Web servers are often the first point of an attack

Key Vulnerabilities:

- Patching, updates, & secure configurations

Cyber Signals of importance:

- Unpatched Common Vulnerabilities & Exposures (CVEs)
- Weak Secure Sockets Layer and Transport Layer Security protocols (SSL/TLS)

Email Security

Key Areas of Cyber Risk

Can lead to Data Breaches, Phishing, and Business Email Compromise

Key Vulnerabilities:

- Misconfigured email servers, open relays
- Weak Spam Detection + Filtering

Cyber Signals of importance:

- Missing or Malformed Sender Policy Framework (SPF) records
- Absence of DKIM and DMARC (DomainKeys Identified Mail + Domain-based Message Authentication, Reporting and Conformance)

Email is a Primary Attack Vector

Remote Access & Virtual Private Network

Key Areas of Cyber Risk

Protecting Access to your Internal Network

Key Exposures:

- Man-in-the-middle Attack
- Stolen Session Tokens

Dangerous when publicly accessible:

- Remote Desktop Protocol
- File Transfer Protocol
- *Anything that has access to sensitive data*

Internet of Things (IoT) Devices

Key Areas of Cyber Risk

The Forgotten Backdoor into Your Network

Key Exposures:

- Country of Origin
- Unpatched Devices

Important to:

- Change Default Credentials
- Patch, Patch, Patch
- Isolate on separate network

Best Practices for Cyber Risk Mitigation

Best Practices

Proactive Risk Mitigation

Building a Strong Defense is Crucial to Cyber Resiliency

- Strong Passwords
- Multi-Factor Authentication (MFA)
- Patch, Patch, Patch

Employee Training

Your first and best line of defense is a group of Engaged, Educated Employees

- Recognizing Phishing + Social Engineering
- Proper Data Handling Practices
- Remote Work Best Practices
- Device Security

Best Practices

Security Controls

The Foundation of Effective Cybersecurity

- Consistency over Everything
- Work smarter, not harder
- Top-down & bottom-up Buy In

Cyber Insurance

Data Breaches & Cyber Incidents can be Extinction-level events

- Cost of Ransom
- Regulatory Requirements
- Remediation
- Loss of Business Income

Questions!

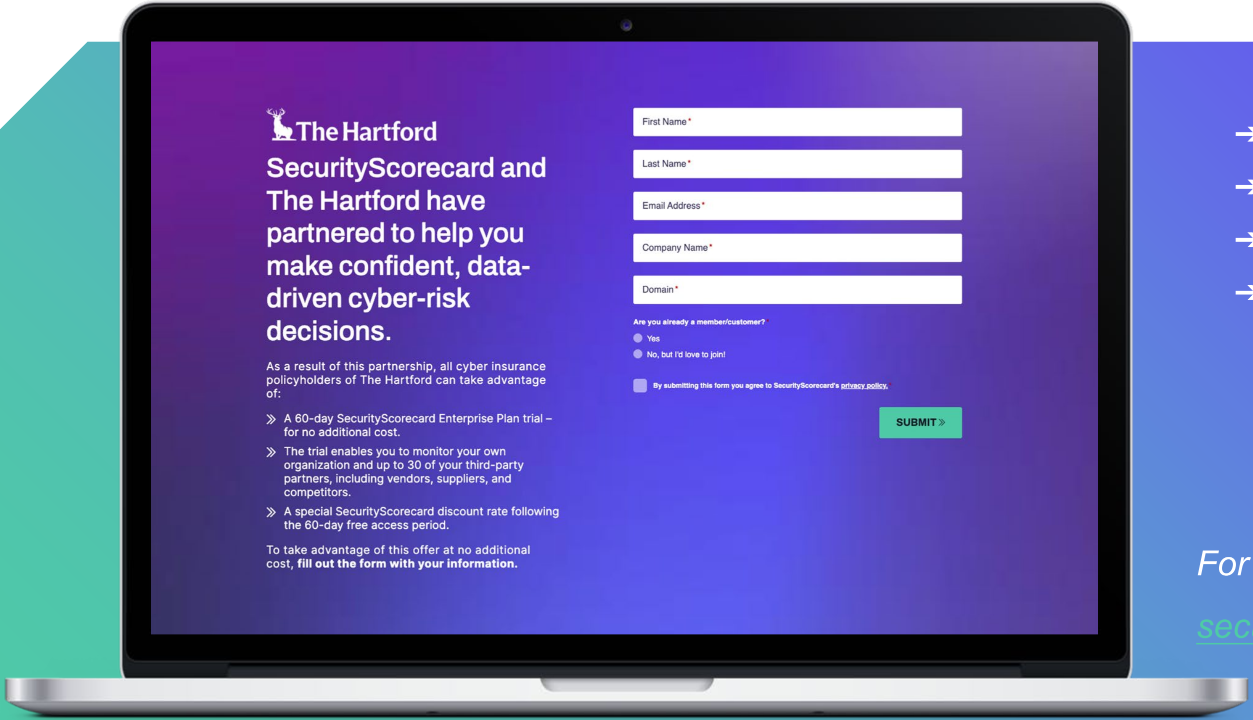
(Ask in Chat)

Your Cybersecurity Journey Starts *Now!*

- Implement These Strategies
- Seek Guidance as Needed
- Contact The Hartford or SecurityScorecard with Any Questions

Andrew Correll
acorrell@securityscorecard.io

SecurityScorecard & The Hartford Have Partnered!



- ➔ A 60-day complimentary Enterprise trial
- ➔ Monitor up to 30 third-parties within period
- ➔ Discounts for Policyholders
- ➔ Forever access to Freemium plan

For more information visit:

securityscorecard.com/the-hartford

Thank you!

Disclaimer