

JUNE 2, 2021

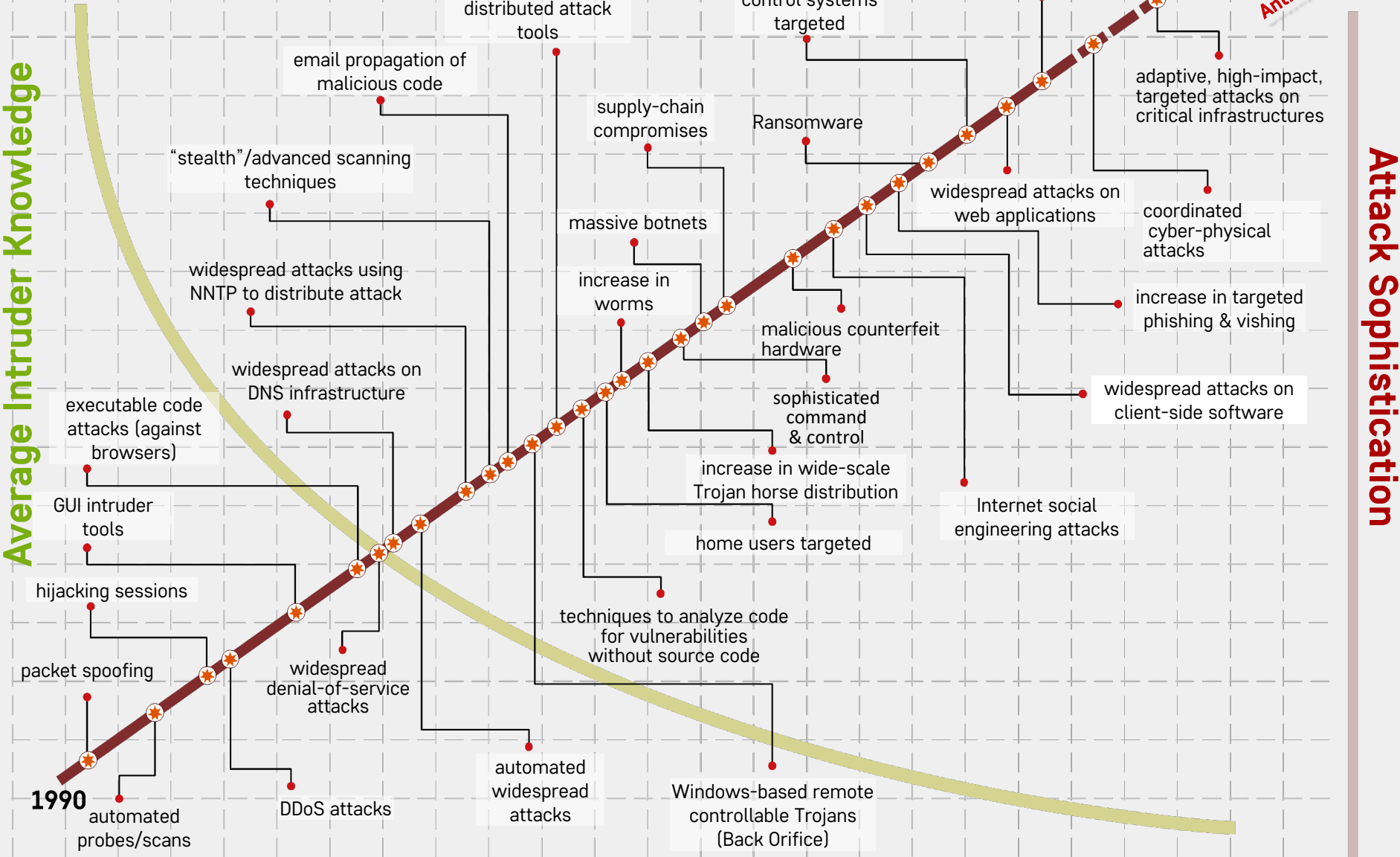


# Risk In The Digital Age

# Global Impacts from Online Crime & Fraud: Majority Are Not Cyber Resilient

- [Crime, Espionage & Fraud](#) - \$945 billion globally in 2020
  - Estimated to be [\\$5.2](#) - [10.5](#) trillion globally by 2025
  - Largest Ransom Payment in 2020 = over [\\$15 million](#)
  - Average Forensic Investigation Cost = [\\$55,960](#)
  - [80%](#) of vendor-caused incidents had notice requirements
  - New LawsUIT Trend → [Supply-Chain Cases](#)
-

# Cyber Threats Over Time

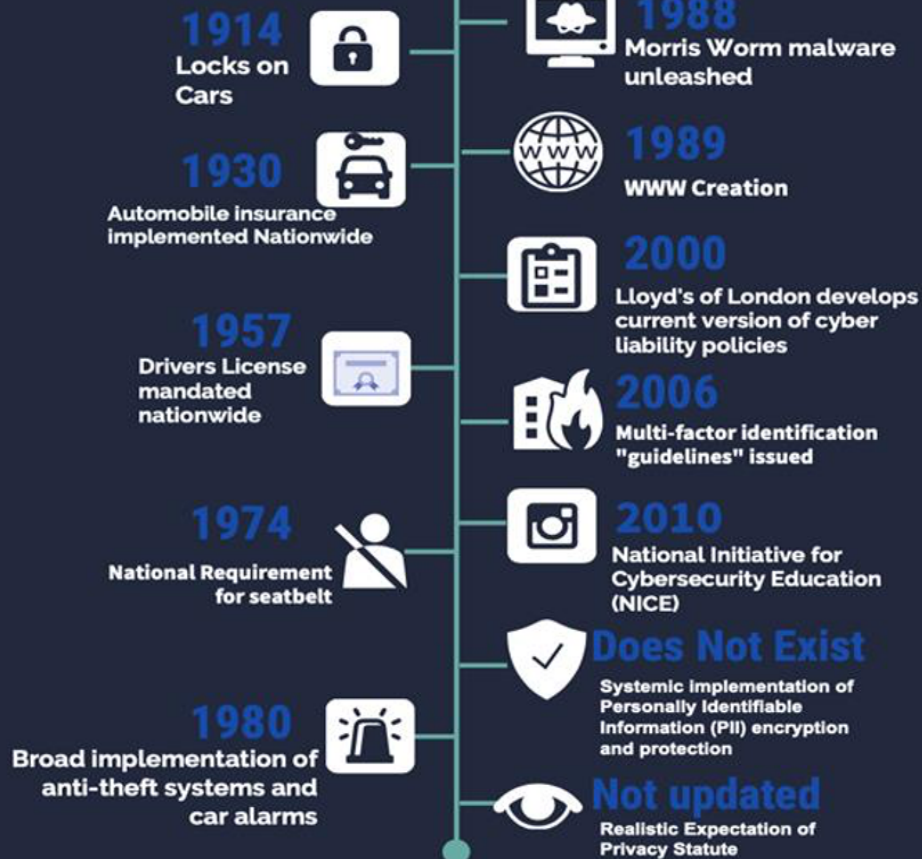


# Physical vs Virtual Security

Timeline of implementations

Automobile Safety & Security Timeline

Cybersecurity Timeline



# Cyber Criminals Follow the Money: Targeting the Most Vulnerable

- A hacker strikes every 39 seconds
- 86% of breaches were financially motivated
- \$17,700 is lost every minute due to a phishing attack
- 65% of criminal groups used spear-phishing (phishing to specific and well-researched targets) as the primary infection vector
- The average cost of a malware attack on a company is \$2.6 million
- The financial services industry takes in the highest cost from cybercrime at an average of \$18.3 million per company surveyed
- The healthcare industry lost an estimated \$25 billion to ransomware attacks in 2019

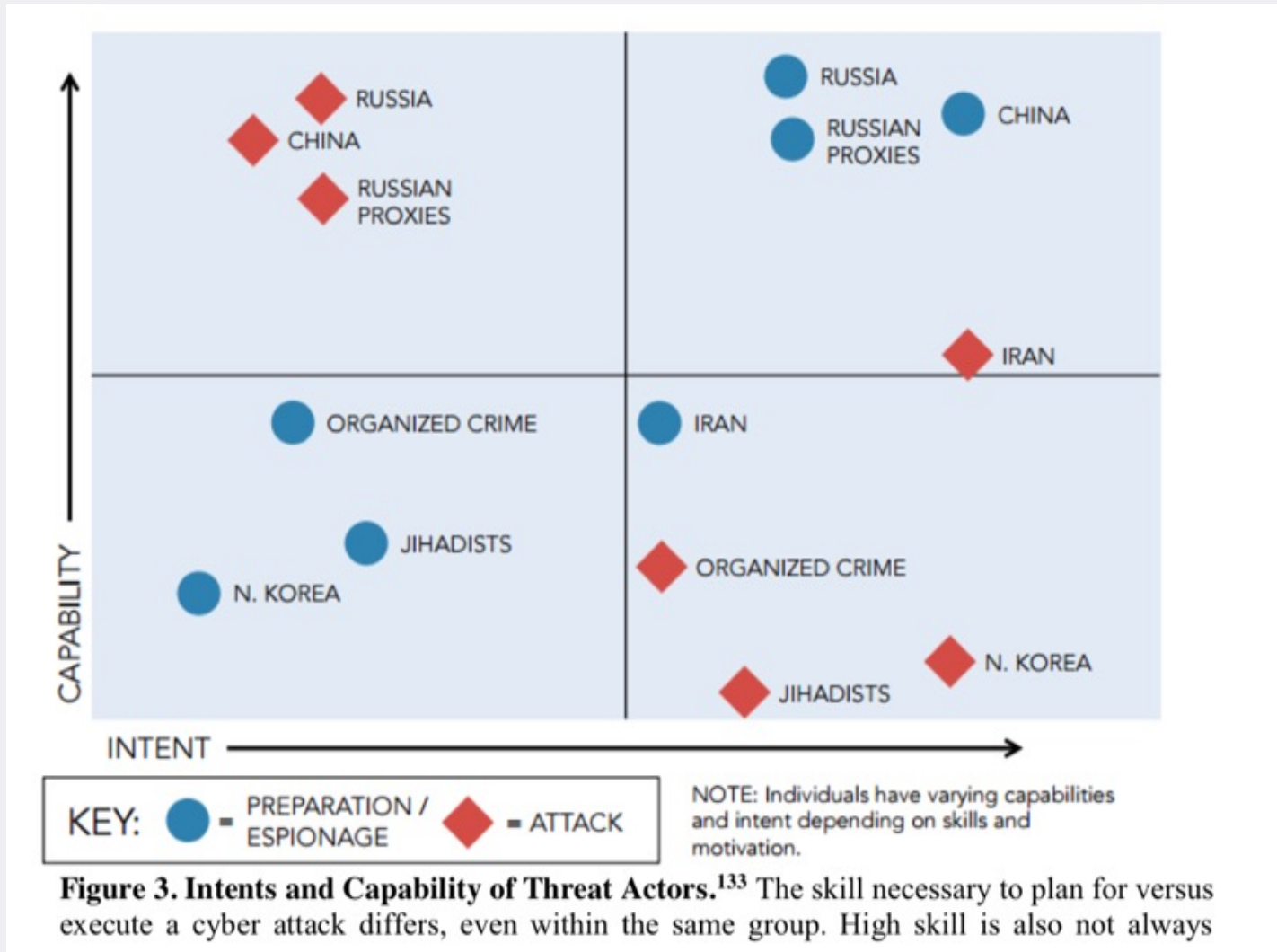
*Cybercrime statistics indicate that every business, no matter the size, is a target*

# Primary Cyber Bad Actors



*Majority are just plain cyber criminals*

# Intentions, Capabilities, and Opportunity



## What is the impact of a cybercrime or fraud event to your Company?

- Businesses and Organizations are at risk daily
- Most do not have in-house cyber risk expertise/CIO/CISO
- Over 70% of cyberattacks target SMBs
- 58% of malware attack victims are categorized as SMBs
- \$200K-\$2M = median loss of fraudulent schemes

*79% of intrusions were crime based in 2020*



## Do you know where to start?

"Doing The Basics" can prevent or mitigate an event:

1. Reduce your Attack Surface through Workforce Cybersecurity Awareness Training
2. Prevent Your IT Systems from being Compromised by having effective automation of System Patching and Email Security
3. Implement communications Encryption and Application Security

*All are available via cost effective and easy to implement SaaS based Solutions*

<https://www.whitehawk.com/marketplace/products>



# Cyber Threat Readiness Questionnaire

- Discover your Sector's Threat Landscape from online crime and fraud
- Build a custom risk profile based on your company's digital footprint

### Cyber Threat Readiness Questionnaire

Answer just 10 questions and find out your top vulnerabilities and get matched to products that can help you today

[What Are the Biggest Threats to Your Industry? Find Out for Free by Answering 10 Questions.](#)

Is your business worth 5 minutes of your time? Answer just 10 questions and find out what the greatest threats to your industry are and how best to protect yourself. Our free online tool identifies your biggest risks and matches you to affordable products that can help you today.

In which industry is your business?

Finance

How many employees does your company have? Include all full time, part time, and contractors.

113

How many users are on your company network? In many cases, this will be the same as the total number of employees.

113

How many office locations does your company have?

4

How many company issued devices (cell phones, computers, iPads, tablets, servers, etc.) does your company own?

248

How extensively does your company use cloud based services?

Substantial

What type of client interactions do you have?

Email  
Face-to-Face  
Managed By A Third-Party Provider  
Mobile  
Phone  
Website

How much web traffic do you receive?

Low

How much does your IT security personnel have of IT security issues?

Moderate

How much of your IT support personnel can provide skilled operational support for the company's networking needs?

None

Submit

# Cyber Risk Profile

## Defend Your Business Against Cybercrime

### Cyber Risk Profile

Industry : Finance  
 Locations : 4  
 Employees : 113  
 Interactions : Email, Face-to-Face, Mobile, Phone, Website

[Retake Questionnaire](#)



Based on the answers provided, your focus should be on protecting your company's computers and users during a wide range of transactions involving many different customers and suppliers. Your business may attract sophisticated groups of attackers, "Advanced Persistent Threats" or "APT", who are willing to invest a lot of time and effort in the hopes of a single large payout. The payout does not have to be financial: cyber criminals may also be targeting your intellectual property. In addition, attackers may see you as a useful stepping-stone in attacking your business partners.

Your company has well-developed plans and instructions for what to do in the event of a security incident. Because of this, make sure that your cybersecurity tools are up-to-date and that you have the necessary resources necessary to identify and address gaps that can be exploited. It is vital to continue to improve and maturing your cyber posture with the use of automation. Implementing high confidence alerts.

Our evaluation indicates that your current overall cybersecurity posture is good. You should take immediate steps to close the most urgent gaps in your cybersecurity.

This profile is based on the small amount of business-specific data you provided in this questionnaire, and on broad statistics for your industry. Please contact us for a more accurate, personalized evaluation.

### Based on your response, below are your solution options

**Balanced**  
 The Balanced bundle offers the cybersecurity products that represent the best practices standard for your company's online operations. This bundle represents what you should be doing.

- DataLocker Encrypted External Hard Drive**  
 Encrypted Storage  
 DataLocker DL3 1TB Encrypted External Hard Drive with RFID Two-Factor Authentication - USB 3.0 External HDD with AES XTS Mode Hardware Data Encryption 1TB w/RFID ENCRYPTION
- Kiwi Syslog Server**  
 Security Information and Event Management  
 Kiwi Syslog® Server is an affordable syslog management tool for network and systems engineers. It receives syslog messages and SNMP traps from network devices (routers, switches, firewalls, etc.), and Linux®/Unix® hosts
- OneConnect Plus 1 Year**  
 Email Filter  
 Advanced spam and malware protection for Exchange with virus scanning and full disaster recovery for a secure email server. GFI OneConnect archives your email and protects your network from email borne threats and costly email downtime.

**Basic Bundle**

The Basic bundle provides the essential cybersecurity products that fit your company's immediate needs. This bundle represents the minimum that your company needs to be doing to prevent or mitigate cyber crime and fraud.

[Review the Bundle](#)

**Balanced Bundle**

The Balanced bundle offers the cybersecurity products that represent the best practices standard for your company's online operations. This bundle represents what you should be doing.

[Review the Bundle](#)

**Advanced Bundle**

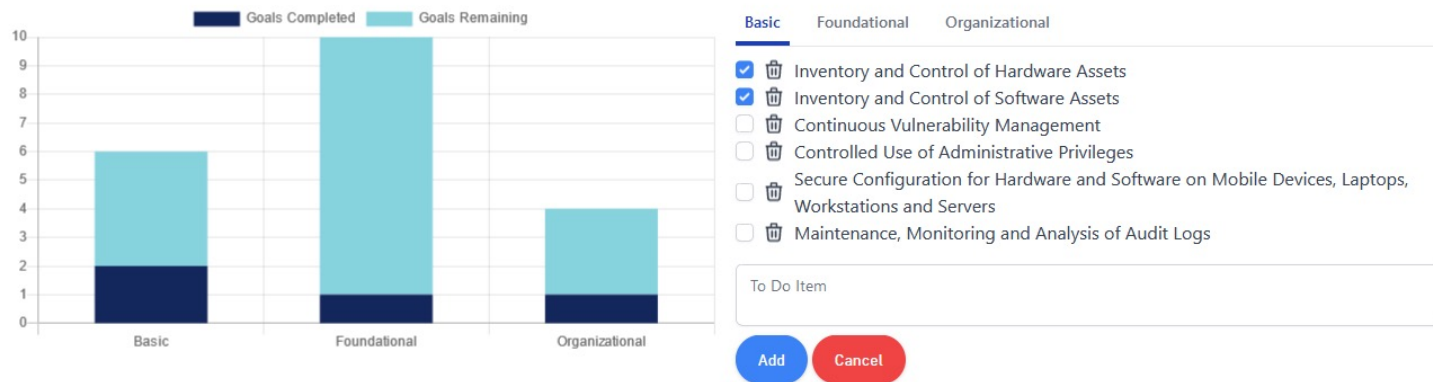
The Advanced bundle is the top of line maturity level for cybersecurity products. This bundle represents the level of cyber maturity that your company should be striving towards to address a breadth of cyber crime and fraud attacks to your revenue, customers and reputation.

[Review the Bundle](#)

Determine the key risks to revenue and reputation, matching commercial solutions to your risk profile

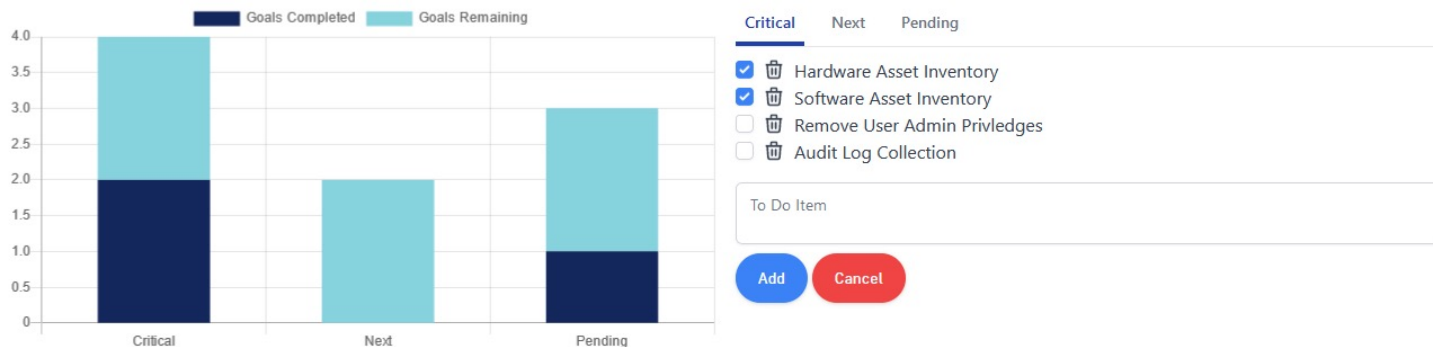
# Maturity Roadmap & Action Plan

Maturity Level Assessment



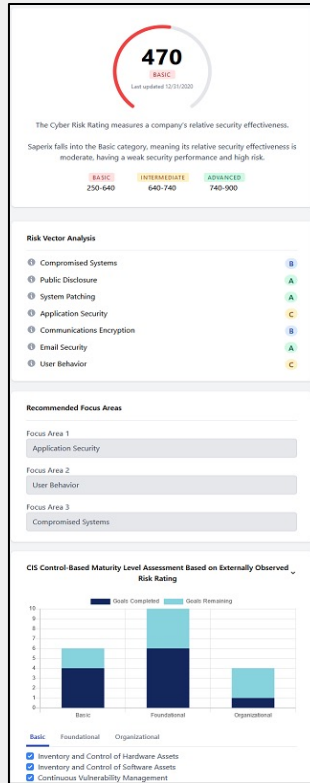
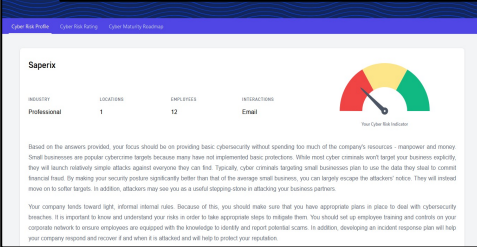
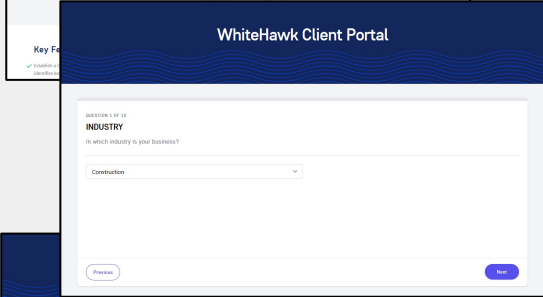
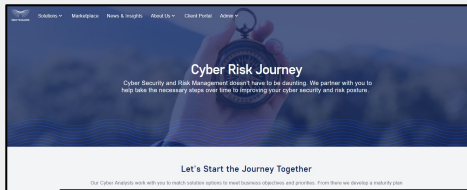
CIS-20 maturity level assessment, based on information gathered during consultation.

Action Plan



Track progress in real-time and set goals using the action plan to monitor cyber maturity.

# Continuous Cyber Risk Monitoring and Prioritization



**Your Mapping to CMMC**  
See the visual below to better understand where each CIS control maps to these new standards. This information is based on externally observed data.

| CIS Control  | #   | CMMC Maturity Levels |       |      |      |
|--|-----|----------------------|-------|------|------|
|  |     | L1                   | L2    | L3   | L4/5 |
| Penetration Tests and Red Team Exercises                       | #20 |                      |       |      | -    |
| Email and Web Browser Protections                              | #7  |                      |       | ●    | ●    |
| Limitation and Control of Network Ports, Protocols, & Services | #9  |                      |       |      | ●    |
| Application Software Security                                  | #18 |                      |       |      | -    |
| Inventory and Control of Software Assets                       | #2  |                      | ●     | ●    | ●    |
| Continuous Vulnerability Management                            | #3  |                      |       |      | -    |
| Controlled Use of Administrative Privileges                    | #4  |                      | ●     | ●    | ●    |
| Maintenance, Monitoring and Analysis of Audit Logs             | #6  |                      |       |      | -    |
| Data Recovery Capabilities                                     | #10 |                      |       |      | -    |
| Secure Configuration for Network                               | #11 |                      | ●     | ●    | ●    |
| Implement a Security Awareness and Training Program            | #17 |                      |       |      | -    |
| Incident Response and Management                               | #19 |                      |       |      | -    |
| Inventory and Control of Hardware Assets                       | #1  | ●                    | ●     | ●    | ●    |
| Secure Configuration for Hardware and Software                 | #5  | ●                    | ●     | ●    | ●    |
| Malware Defenses   | #8  | ●                    | ●     | ●    | ●    |
| Boundary Defense   | #12 | ●                    | ●     | ●    | ●    |
| Data Protection  | #13 |                      |       |      | -    |
| Controlled Access Based on the Need to Know                    | #14 | ●                    | ●     | ●    | ●    |
| Wireless Access Control  | #15 | ●                    | ●     | ●    | ●    |
| Account Monitoring and Control                                 | #16 | ●                    | ●     | ●    | ●    |
|  |     | 7/8                  | 10/16 | 4/19 | 0/20 |

| Symbol | Meaning                           |
|--------|-----------------------------------|
| ●      | Meets or exceeds all expectations |
| ●      | Meets some expectations           |
| ●      | Has significant shortfall         |

Data Ingestion

Risk Rating Analysis

Map to Frameworks

Initiate

Evaluate

Inform

# Cyber Risk Consultation, Scorecard, and Action Plan



**WHITEHAWK**

## Cyber Risk Scorecard

On Company: Sample Company

| Company  | Domain  | # IP Addresses  | Monitored by            |
|--|---|---|-------------------------|
| Sample Company   | SampleCompany.com   | 2003  | 7 Entities              |
| <b>Security Rating</b>   |   | <b>Risk Vector Performance</b>  |                         |
| Ratings measure a company's relative security effectiveness.   |   | Risk Vector grades show how well the company is managing each risk vector.  |                         |
| <b>610</b>   | Advanced: 900 – 740   | Compromised Systems: A  | System Patching: A      |
|  | Intermediate: 740 – 640   | Communications Encryption: D  | Application Security: F |
|  | Basic: 640 – 250  | User Behavior: A  | Email Security: A       |
| <b>Prioritized Areas of Focus</b>  |   |   |                         |
| WhiteHawk Cyber Analyst has identified top-3 Focus Areas the company should consider   |   |   |                         |
| Focus Area 1:  | Application Security  |   |                         |
| Focus Area 2:  | Communications Encryption   |   |                         |
| Focus Area 3:  | Compromised Systems   |   |                         |
| <b>Solution Options</b>  |   |   |                         |
| Solution options that address primary business risks identified in the Cyber Risk Scorecard. Alternatives for each are included in the product details section |   |   |                         |
| <b>Essential Bundle</b>  | <b>Balanced Bundle</b>  | <b>Premier Bundle</b>   |                         |
| <ul style="list-style-type: none"> <li>- AppSec Labs: AppUse Pro</li> <li>- Micro Focus Software Inc.: Identity Manager Advanced Edition</li> </ul>            | <ul style="list-style-type: none"> <li>- SecuDrive: SecuDrive File Server</li> <li>- SolarWinds: Network Performance Monitor</li> <li>- BoldonJames: Office Classifier</li> </ul> | <ul style="list-style-type: none"> <li>- Check Point: Threat Prevention Security Suite</li> <li>- Fortinet: FORTIANALYZER-3900E LOG &amp; ANALYSIS APPL</li> <li>- Trusted Internet, LLC: Student Cyber Protector</li> <li>- SolarWinds: Web Performance Monitor</li> </ul> |                         |
| For more solution options, visit <a href="http://www.whitehawk.com/marketplace">www.whitehawk.com/marketplace</a>  |   |   |                         |

### Maturity Level Assessment



| Maturity Level | Goals Completed | Goals Remaining |
|----------------|-----------------|-----------------|
| Basic          | 2               | 4               |
| Foundational   | 1               | 9               |
| Organizational | 1               | 3               |

- Inventory and Control of Hardware Assets
- Inventory and Control of Software Assets
- Continuous Vulnerability Management
- Controlled Use of Administrative Privileges
- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- Maintenance, Monitoring and Analysis of Audit Logs

To Do Item

Add Cancel

---

### Action Plan



| Action Plan Category | Goals Completed | Goals Remaining |
|----------------------|-----------------|-----------------|
| Critical             | 2.0             | 2.0             |
| Next                 | 0.0             | 2.0             |
| Pending              | 1.0             | 1.0             |

- Hardware Asset Inventory
- Software Asset Inventory
- Remove User Admin Privileges
- Audit Log Collection

To Do Item

Add Cancel

WhiteHawk Cyber Risk Scorecard

Maturity Model & Action Plan

Engage

Monitor

## Take Smart Action: To Mitigate Your Cyber Risks

- Everyone is a target
- Criminals are following the money and social media enables their focused targeting of your business or organization's members
- Knowing your key Cyber Risks is now an imperative
- Know your top 5 Risks & Mitigate them today
- Implement for one year and track your maturity & resilience

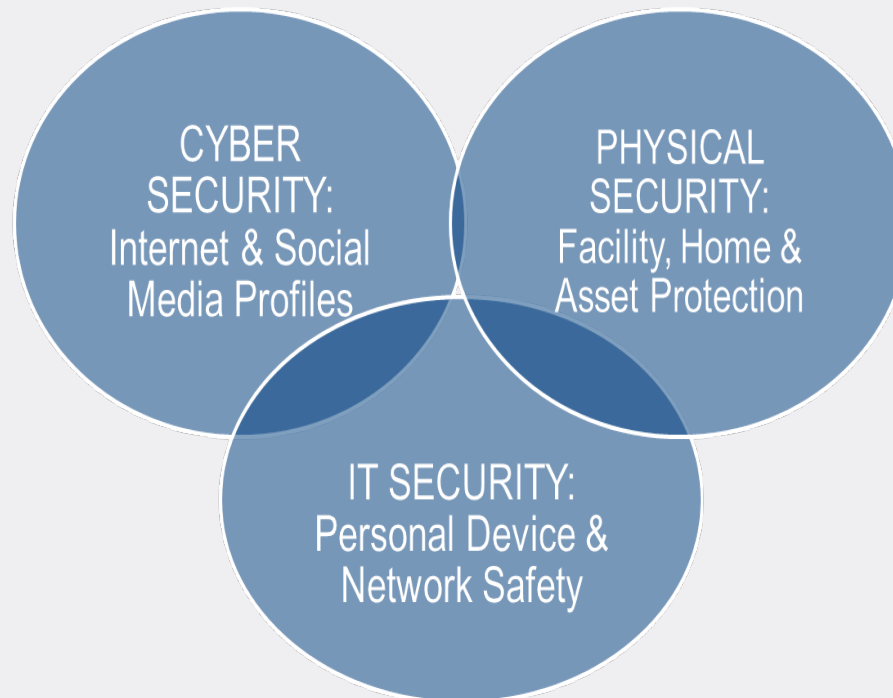


# Your Personal Approach to Social Media Security



## Think 360 Security

It is impossible to separate social media from the larger picture of security – all are mutually inclusive:



## A Pragmatic Perspective:

- Have a healthy dose of paranoia
- Always expect that bad guys may want to get at me or my company
- Keep a low profile at home and abroad
- Be private about my movements
- Be aware of my surroundings always
- Take precautionary measures
- Live my life and work to the fullest - but always be aware

## Personal Disclosure and PII:

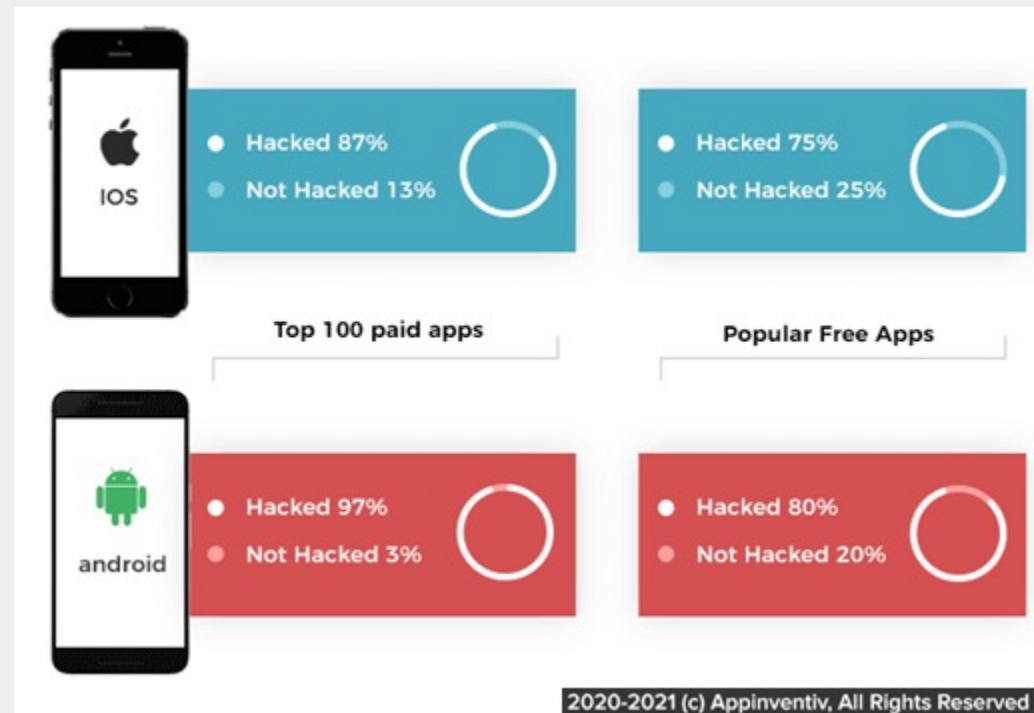
Most social media sites will ask for personal information to be included in your profile or during account registration.

- Do not post DOB, phone numbers, email addresses, home addresses.
- Decide whether you want to use your “true name,” a nickname, or an alias.
- Decide whether you want to use a headshot, other picture, or no photo.
- Choose a password that you do not use for other online activities or to login to your computer/devices.

# Phone and Tablet Apps: What are they collecting?

- Location tracking
- Accessing the device's address book or contact list
- Single sign-on via social networks
- Identifying the user or the phone's unique identifier (UDID)
- Number and type of in-app purchases
- Number of times used a browser, dialed a phone #

## Percentage of Hacks in Paid vs Free Apps



# Social Media: Assistance for Settings

Facebook Help Center for Settings

<https://www.facebook.com/help/193677450678703>

Consumer Reports – How to Use Facebook Privacy Settings

<https://www.consumerreports.org/privacy/facebook-privacy-settings/>

Step by Step Instructions

<http://facecrooks.com/Internet-Safety-Privacy/how-to-lockdown-your-facebook-account-for-maximum-privacy-and-security.html/>

YouTube Video - Facebook Settings

[https://www.youtube.com/watch?v=Ui\\_v5Gb8A54](https://www.youtube.com/watch?v=Ui_v5Gb8A54)

# Cybercrime Support Network (CSN)



## Report. Recover. Reinforce.

The Cybercrime Support Network was established to give a voice to cybercrime victims and support a coordinated response from federal, state and local law enforcement to manage cybercrime incidents affecting individuals and small businesses.

CSN is piloting US programs to utilize existing referral infrastructure and the website fraudsupport.org to facilitate cybercrime reporting, response and recovery.

Through a partnership between WhiteHawk and CSN, small and midsize businesses (SMBs) that contact CSN in need of cybercrime and fraud response and mitigation services will be provided incident response resources including WhiteHawk.

## Cyber Intelligence Sharing

Continuously Working Across Your Business Sector, Government Sector and Community (Models: ISACs & Cyber Threat Alliance)





# GLOBAL CYBER ALLIANCE



## Do Something. Measure It.™

The Global Cyber Alliance (GCA) is an international, cross-sector effort dedicated to reducing cyber risk and improving our connected world.

"Our vision is a secure, trustworthy Internet that enables social and economic progress. Realizing this vision requires tackling a big problem: reducing cyber risk. We approach this challenge by building partnerships and creating a global community that stands stronger together. We tackle projects that will have a global impact, are scalable, measurable, and will reduce risk."

Through the combined efforts of WhiteHawk and GCA, small and midsize businesses (SMBs) that contact GCA in need of cybercrime and fraud response and mitigation services will be provided incident response resources including WhiteHawk.

# How Does Anyone Keep Up with Cybersecurity Solutions?

The image displays a comprehensive grid of cybersecurity solutions, organized into 20 distinct categories. Each category is represented by a dark header bar with the category name, followed by a collection of logos for leading companies in that space. The categories and their associated companies are as follows:

- Infrastructure Security**: Network Firewall (Cisco, Palo Alto, Juniper, etc.), Network Monitoring (NetScout, Juniper, etc.), Intrusion Prevention Systems (Cisco, Palo Alto, etc.), Unified Threat Management (Palo Alto, Fortinet, etc.).
- Endpoint Security**: Endpoint Prevention (Kaspersky, Trend Micro, etc.), Endpoint Detection & Response (CrowdStrike, SentinelOne, etc.).
- Application Security**: WAF & Application Security (Akamai, Cloudflare, etc.), Vulnerability Assessment (Bugcrowd, Rapid7, etc.).
- Managed Security Service Provider**: IBM, Verizon, Optiv, etc.
- Messaging Security**: Microsoft, Cisco, etc.
- Web Security**: Blue Coat, Cisco, etc.
- IoT Security**: MOCANA, Argus, etc.
- Security Operations & Incident Response**: SIEM (Splunk, LogRhythm, etc.), Security Incident Response (Palo Alto, etc.).
- Threat Intelligence**: BrightPoint, DomainTools, etc.
- Mobile Security**: Lookout, Avast, etc.
- Data Security**: Veracode, etc.
- Transaction Security**: Fortra, etc.
- Specialized Threat Analysis & Protection**: FortScale, etc.
- Identity & Access Management**: Okta, etc.
- Risk & Compliance**: RedSeal, etc.
- Cloud Security**: Palo Alto, etc.

# Key Cyber Risks and Solutions

## Financial Fraud, Identity Theft and Mobile Security

Financial identity theft is a significant crime, and potentially one of the more damaging types of identity theft. Below are some solutions that address these risks.

EZShield/WH SaaS <http://mydefense.ezshield.com/whitehawk>

Cleafy <https://www.cleafy.com/>

Clearforce- <https://clearforce.com/>

## Password Lock Boxes / Password Managers

A password manager can dramatically reduce the risk of credential theft, as a result weak or reused password. There are 2 non-Apple options which can address this risk and provide protection:

Roboform - <https://www.roboform.com/>

OneLogin - <https://www.onelogin.com/>

## Secure Communications (email, texts, Telcons)

Maintaining secure communications, is an essential part of protecting an organization's reputation, its customers' sensitive information, its compliance with government regulators—and, ultimately, the company's bottom line.

Preveil - <https://www.preveil.com/>

DekkoSecure- <https://www.dekkosecure.com/>

Mimecast- <https://www.mimecast.com/>

# Key Cyber Risks and Solutions, cont.

## Cyber Event Response, Forensics & Mitigation

Critical that a business can identify and respond to a breadth of cyber events, having a relationship in place.

Malwarebytes - <https://www.malwarebytes.com/>

Rendition Infosec - <https://www.renditioninfosec.com/>

For Larger Businesses/Organizations: Response services from CrowdStrike

<https://www.crowdstrike.com/>

## Cybersecurity Awareness Training

90% of all events are the result of employee actions. Two industry leaders are:

KnowBe4 - <https://www.knowbe4.com/>

Virescit Tactical Systems - <https://vtscyber.com/>

## ISP & MSP Impactful Security Features

These are ISP and MSP features that can strengthen your cyber posture – *but also ask your current MSP about their security features:*

Red Sky Alliance - <https://www.wapacklabs.com/redxray>

Alienvault, now ATT Cybersecurity - <https://www.alienvault.com/>

# Sontiq/WH Business Suite: Overview



Sontiq is the combination of EZShield and IdentityForce. These two identity security powerhouses coming together allows for strength in data protection. Sontiq aims to provide customers the opportunity to grow and develop their Business in a way that allows them to be protected from risks without having to be restricted in their potential for connection. Visit <https://www.whitehawk.com/business-risk-suite> to enroll today.

## Key Features:

- Company ID Restoration Pro
- Online Identity Vault
- Password Manager
- Personalized Identity Reports
- Security Self-Assessment
- Breach Readiness Toolkit
- Discounted Employee Benefit & Breach Victim Services
- Fully-managed identity restoration
- Live support M-F 8am - 8pm EST
- Mobile Defense Suite - Mobile Attack View, Control and Recovery
- Dark Web Monitoring - Detect fraudsters trading your information on the Dark Web.