# Physical vs Virtual Security & Safety

<table>
<thead>
<tr>
<th>Automobile Safety &amp; Security Timeline</th>
<th>Cybersecurity Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td>o Locks on cars - 1914</td>
<td>o Morris Worm malware unleashed - 1988</td>
</tr>
<tr>
<td>o Nationwide implementation of Automobile Insurance - 1930</td>
<td>o WWW creation – 1989</td>
</tr>
<tr>
<td>o Nationwide Interstates – 1956</td>
<td>o Lloyd's of London develops current version of cyber liability policies - 2000</td>
</tr>
<tr>
<td>o Drivers Licenses mandated nationwide - 1959</td>
<td>o Multi-factor identification “guidelines” issued - 2006</td>
</tr>
<tr>
<td>o Widespread teaching of Driver Education - 1965</td>
<td>o National Initiative for Cybersecurity Education (NICE) 2010</td>
</tr>
<tr>
<td>o National requirement for seatbelts - 1974</td>
<td>o Systemic implementation of Personally Identifiable Information (PII) encryption and protection – does not exist</td>
</tr>
<tr>
<td>o Broad implementation of anti-theft systems and car alarms - 1980</td>
<td>o Realistic Expectation of Privacy Statute – has not been updated</td>
</tr>
</tbody>
</table>
Primary Cyber Bad Actors
Figure 3. Intents and Capability of Threat Actors. The skill necessary to plan for versus execute a cyber attack differs, even within the same group. High skill is also not always
Cyber Threat Over Time

- **1990**
  - Automated probes/scans
  - DDoS attacks
  - Executable code attacks (against browsers)
  - GUI intruder tools
  - Hijacking sessions
  - Packet spoofing

- **2018**
  - Anticipated attacks
  - Persistent malware infiltration & persistent surveillance
    - Control systems targeted
    - Increase in targeted phishing & vishing
  - Widespread attacks on client-side software
  - Widespread attacks on web applications
  - Coordinated cyber-physical attacks

- **Average Intruder Knowledge**
  - Ransomware
  - SMB
  - Increase in targeted phishing & vishing
  - Internet social engineering attacks

- **Techniques**
  - Email propagation of malicious code
  - "Stealth"/advanced scanning techniques
  - Widespread attacks on DNS infrastructure
  - Executable code attacks (against browsers)
  - GUI intruder tools
  - Hijacking sessions
  - Packet spoofing
  - DDoS attacks
  - Automated probes/scans
  - Supply-chain compromises
  - Massive botnets
  - Increase in worms
  - Malicious counterfeit hardware
  - Sophisticated command & control
  - Increase in wide-scale Trojan horse distribution
  - Home users targeted
  - Techniques to analyze code for vulnerabilities without source code
  - Persistent malware infiltration & persistent surveillance
  - Windows-based remote controllable Trojans (Back Orifice)
Cyber Criminals are Targeting SMBs Daily

Cybercrime damage will cost businesses across the globe over $3 trillion by 2020.

- 58% of victims are SMBs
- 92% of malware delivered by email
- 2x increase in attempted attacks against IoT devices
- $US7.91 MM, up 29% since 2013
- Average SMB paid $4.13 MM in loss of customers due to breaches
- 81% of SMB’s reported some kind of cyber event

Sources:
1. Juniper Research
2. Verizon Data Breach Investigations Report (DBIR)
3. IBM & Ponemon Institute
4. Symantec
How Does Anyone Keep Up with Cybersecurity Solutions?
According to 2018 Market Research:

Clients will not put basic cybersecurity practices and solutions in place (even if they are regulated) unless:

1. They experience a cybercrime or fraud event
2. Have a contract at risk with a government or industry customer
3. Or are otherwise enabled and it is affordable and easy.

Major Industries (Banks, Insurance, Employers) can demonstrate their commitment to their Customers by:

Providing effective, low cost, easy to implement cybersecurity risk ratings and mitigation services.
What Can You Do?

• **Determine What You Need To Protect First**: Intellectual property, customer/employee information, financial data, etc. - keep IP offline or encrypt it

• **Keep Up With The Technology**: Software upgrades, IT security patches, passwords and protocols

• **Know the Current Cybercrime and Fraud Trends**

• **Be an Active Consumer**: Demand assurance, protection and additional security measures from your service or product providers. Start with your Home Office!

• **Establish A Relationship With Your Local InfraGuard**
  www.infragard.org
Establishing:

A Cyber Risk Baseline & Response Plan
In order to Manage Cyber Risk, you need to know your cyber baseline

This basic cyber risk profile survey assesses across the portfolio and industry to understand common attacks and mitigation needs.

• The questions in this survey are used to understand the mindset related to cybersecurity and common pain points. Results of the survey will be provided back to you.

• Course Survey

• The information you submit in this survey is anonymous and will be used to provide an analysis snapshot of the threat trends.

• Please take 5-10 mins to complete this survey and we will review during the last class today.
Biggest Cybersecurity Risks

Contribution Data

• Without basic data protections, proprietary data could be exposed/stolen/tampered with by criminal or competitor
• 60% of small businesses close their doors within six months of a data breach

Foundation Intelligence

• Unencrypted emails and files could give determined competitor a Family Foundation advantage
• Global annual cybercrime costs will grow from $3 trillion USD in 2015 to $6 trillion USD annually by 2021 (includes damage and destruction of data, theft of intellectual property, and disruption)
Recommendations

Based Upon:

- Emerging technology
- Latest sector and at large cyber threat vectors
- Pain points to industry and cyber vulnerability
- Internationally recognized best practices (ISO Standards, NIST-CIS Controls and FBI)
#1: Implement Access Control
- Implement multi-factor authentication for device (computer and mobile), network, and application (email or other collaboration tools) access

#2: Secure Your Network
- Safeguard your Internet connect with the latest firewall technology
- Secure remote access into your corporate network with a Virtual Private Network (VPN)
- Implement encrypted voice over internet protocol (VoIP) phones and conference lines to protect voice communications

#3: Prevent Malware
- Implement the latest anti-malware technology
- Ensure software updates are made automatically

#4: Backup Your Family Foundation Data
- Encrypt sensitive data to promote integrity and confidentiality of Family Foundation intelligence
- Automatically backup your most sensitive data at least weekly
- Ensure backups are stored in a location not connected to your company network

#5: Conduct IT Architecture Review
- Partner with a trusted consultant to independently assess your current IT architecture and recommend cost-effective solutions and configurations for your business

### Summary of Recommendations
### Summary of Recommendations

<table>
<thead>
<tr>
<th>#6: Assess Third Parties</th>
<th>• Partner with a trusted consultant that can independently assess your investment targets and partner companies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>#7: Establish Company Security Policies</strong></td>
<td>• Establish policies on how employees should handle and protect Family Foundation data. Clearly outline the consequences for violating your business’s Cybersecurity policies</td>
</tr>
<tr>
<td><strong>#8: Educate Employees on Cyber Threats</strong></td>
<td>• Partner with a trusted expert to educate your employees about online threats and how to protect your Family Foundation data</td>
</tr>
<tr>
<td><strong>#9: Antivirus and backup</strong></td>
<td>• Routinely backing up your information and using antivirus to check devices for any unusual activity.</td>
</tr>
<tr>
<td><strong>#10: Mobile Attack control</strong></td>
<td>• Protecting your information when you or anyone from your family office is on the go. Mobile devices connecting to foreign networks can pose a risk to more cyber attacks.</td>
</tr>
<tr>
<td><strong>#11: Financial Fraud Protection</strong></td>
<td>• Taking precautionary steps to secure your finances by securing who has access to your information and verifying their identification</td>
</tr>
<tr>
<td><strong>#12: Identity theft protection</strong></td>
<td>• Family offices and their employees can be at risk of malicious cyber attackers stealing the identity of authorized personnel and using it to access sensitive information or act maliciously on their behalf. Being proactive in protecting all identities is imperative in keeping all information secure</td>
</tr>
</tbody>
</table>
Who’s Watching Your Back Door: Insider Risk

• Anyone with Access
• Contractors
• Partners
• Indiscreet Family & Friends
• Home Office Exploits:
  https://www.whitehawk.com/robertsreport_homeofficesecurity
Small Business SaaS Suite | Cyber Risk Details

Company Profile

Overview  Risk Rating  Maturity

Omni Delta, Inc.

Industry: Arts  Locations: 8
Employees: 50  Interactions: Email, Mobile, Phone

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 balances necessary internal rules against a desire to foster individual solutions. Because of this, you should make sure that your cybersecurity tools are up-to-date and providing the detail necessary to identify and address potential gaps that could be exploited. Identify industry and internal risks and then take steps to mitigate them. Create an incident response plan if your company does not already have one. Know your compliance requirements, and maturity plan to take your cybersecurity program to the next level.

Our evaluation indicates that your current overall cybersecurity posture is poor. Your company needs to 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 have provided through the questionnaire, and on broad statistics for your industry. Please contact Whitetail to get a more accurate, personalized evaluation.

Solution 1 - 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.

Solution 2 - 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.

Solution 3 - 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.
Cybercrime Support Network (CSN)

fraudsupport.org powered by: cybercrime
SUPPORT NETWORK


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)
“Reasonable Expectation of Privacy” in the Digital Age?

1) Work Emails – No

1) Social Media Postings – No

2) Searching and Shopping On-Line – No

3) Blogging – No

4) Communications that impact a potential crime or terrorism act (with probable cause) – No

1) Cell Phone conversations (Device owned by you in private place) – Yes

2) Personal Emails on your personal infrastructure – Yes

3) Legal Financial Transactions – Yes

4) Personal Medical Information – Yes

5) Legal Council – Yes

6) Proprietary or Patented IP - Yes
Court Precedence: Using 19th & 20th Century Statute in the Digital Age

Katz v. United States, 1967

Issue: Wiretapping and Expectation of Privacy

- The Fourth Amendment protects people, not places

- Since Katz, the use of computers, cell phones, personal digital assistants, and other wireless devices has created new kinds of searches and applications of the Fourth Amendment
How Does This Case Apply to Private Persons?

With the current law, a person must demonstrate two things to establish a reasonable expectation of privacy:

1) That the individual has a subjective expectation of privacy;
2) That the subjective expectation of privacy is one that society is prepared to recognize as reasonable
Let’s Get to the Next Level of Discussion & Solutions! Many Current Statutes & Policies are out of date

Let’s Bring Pragmatic Laws & Practices to: The Current Wild West
Your Personal Approach to Social Media Security

MANAGING YOUR DIGITAL FOOTPRINT

Personal Information
Family Information
3rd Party Disclosure
Reputational Risk & Image
Erroneous Information
Social Media

Manage risk by understanding the 5 “P’s” of Social Media Security:

• Purpose
• Personal Disclosure & PII
• Privacy
• Photos & Videos
• Propagation
Think 360 Security

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

- **Cyber Security**: Internet & Social Media Profiles
- **Physical Security**: Facility, Home & Asset Protection
- **IT Security**: Personal Device & Network Safety
A Pragmatic Perspective:

- Have a healthy dose of paranoia
- Always expect that bad guys may want to get at me or my family or my SMB
- 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
A Personalized Approach:

No Facebook Presence vs. Limited Facebook Presence - Offline Sharing
Groups
No broad announcements of where I am or where I am going...

No open sharing of small children’s photos in open social media

No LinkedIn Account vs. limited personal/professional data exposure
No personal social media engagement (Twitter, etc.) except as my Company
Sensitive SMB communications are encrypted and never public – SMB deals, trips, impending financial transactions

Put thought into your approach...
Social Media

Assistance for Settings:

Facebook Help Center for Settings
https://www.facebook.com/help/193677450678703

Good Read on Wired.com

Step by Step Instructions

YouTube Video - Facebook Settings
https://www.youtube.com/watch?v=Ui_v5Gb8A54
As an SMB or Individual in a Netted World:

- Be aware - If there is gain to be made, there is a criminal target
- Today’s criminals have access to your Company and Individual Information
- You, your company team, your family members can be targeted at any time
- Be Engaged - Be a Security Consumer
Leverage Social Media in Support of Your Company’s/Organizations Objectives:

- Why are you using social media?
- Which platforms do you want to use?
- Do you want to interact with professionals or family & friends?
- How much time do you envision spending on social media?
- What devices do you want to use to access your social media?
Phone and Tablet Apps: Access to Social Media

App Risk – 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 number

EXAMPLE: Facebook Session Hijacking Blog
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.
Privacy Settings

- Manage privacy settings on the chosen social media sites.
- Manage privacy settings on your devices (i.e., iPhones, iPads, Android smartphones).
- Maintain your privacy by re-visiting privacy settings each time the social media site provides updates or a new version.
Photos & Videos

• Photos (and videos) may contain GPS location information and time/date stamps.
• Manage location data by understanding the settings on your device(s).
• Photos (in Facebook) can be “tagged” – decide whether you want to allow tagging.
Propagating your account(s) with strict privacy and security settings can mitigate information propagation.

Others, however, can post what they hear or what they see. You cannot control all of the information on social media.

The Internet (databases, real estate sites, people-find sites, and genealogy sites) have already disclosed information about you.
Registering a new Account on Social Media

Use a strong password different from the passwords you use to access other sites.

If you are asked to provide security questions, use information that others would not know about you or cannot easily look up on alumni sites, LinkedIn or public databases.

Never provide a work-associated email to a social network, especially when signing up. Consider creating a new email address strictly to connect with your social networking profile(s). Use a “throw-away” Gmail address or something similar.

Consider not using your real name, especially your last name. Be aware that this may violate the terms of service of some social networks.

Provide only information that is necessary or that you feel comfortable providing. When in doubt, err on the side of providing less information. Remember, you can always provide more information to a social network, but you can’t always remove information once it’s been posted.

Be sure to keep strong antivirus and malware protection on your computer.
Facebook and LinkedIn

- Don’t mix “SMB& pleasure” – have separate accounts for your personal life and your corporate life. For personal use, you may want to use an alias, nickname.
- Every time there is an update or new version released, you must re-set all of your privacy and use settings.
- People tend to gather information from Facebook and LinkedIn.
- Inter-connecting apps also link Facebook and LinkedIn.

- Reveals Your Rolodex…didn’t we used to protect those?
- May “tip-off” your company based on who is in your contacts lists and who you have added.
- Even if it is “private”…shoulder-surfing and other means of seeing the information is possible (LinkedIn owns SlideShare, where your data can also inadvertently be revealed).
- If you are surfing LinkedIn, those you look up could know that you are clicking on their profiles.