How can you safeguard your business from Cyber risks being cost conscious?

Sep 17, 2025

Agenda

1. Quick Intro
2. Cyber Risks Around You
3. Protecting Small businesses
4. Protecting High Networth Investors
5. Protecting Online Shoppers
6. Q&A and Takeaways

Raise your awareness on cyber risks impacting businesses and individuals

What is this session about?

Intended Audience

1. Small to Medium sized Business Owners
2. High Net Worth Individuals
3. Online shoppers
4. Corporate workers

What can you expect from this session?

1. **LEARN** about cyber risks impacting SMBs
2. **UNDERSTAND** how these risks impact your professional and personal lives
3. **TAKE AWAY** some practical tips to apply immediately to protect yourself and your businesses, <u>cost effectively</u>

Ravi Viswanatthan

Scan on your phone

ABOUT ME

28+ YEARS IN CYBERSECURITY, COMPLIANCE, RISK GOVERNANCE, DATA PRIVACY IN LARGE GLOBAL FORTUNE 100s

Current

- Products Security Head, Payments Security, Amazon
- Board Advisor to Swiftsecurity.AI, Vation Ventures, Glilot Capital Partners
- **Own a security consulting firm: Wersec.com**

Former

Director of Cybersecurity, Bank of Montreal
Sr Mgr, Product Cybersecurity, Abbott

FAMILY

- **Born and raised in Chennai, INDIA**
- **Chicago native for the last 20 years.**
- **Wife and I have two teenage kids**

HOBBIES

- **Avid Backpacker and Camper**
- **Bikram Hot yoga practitioner for 10 years**
- **You need a volunteer for a good cause? Call me**

Let's talk about cyber risks on sensitive data

What is Sensitive data?

01 **ONLINE SHOPPERS**

Name, address, Phone #, Credit card #s, Your medical data, Banking data, Gift card #s

02 **BUSINESS OWNERS**

Name, Address, Phone #, Date of Birth, Social Security numbers, Credit card #s, Employment / Immigration / work authorization info

03 **HIGH NET WORTH INDIVIDUALS**

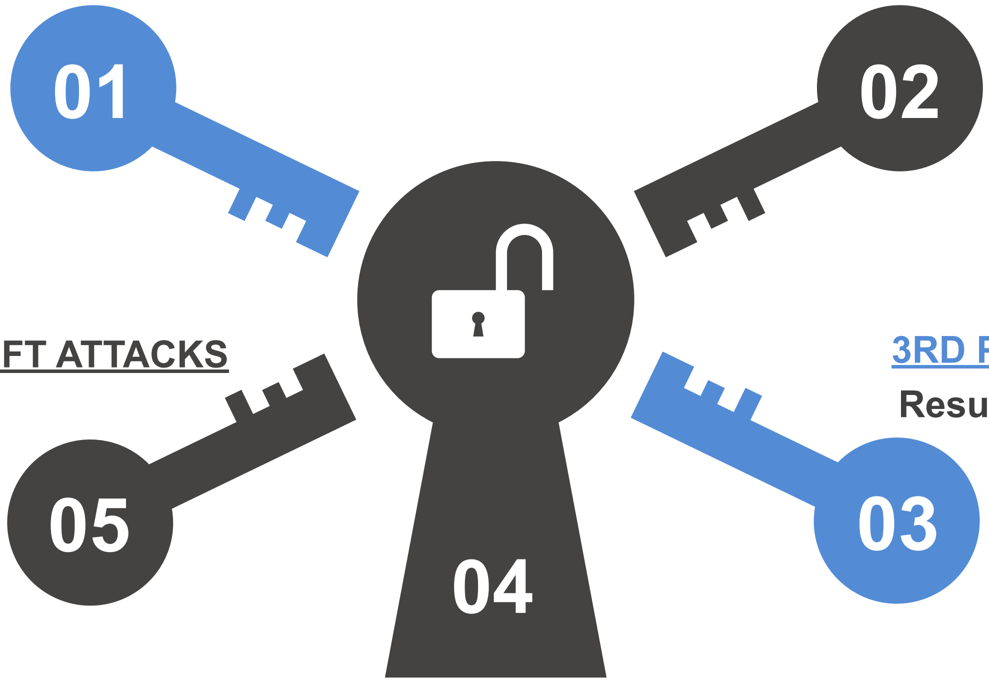
Retirement accounts, Tax returns, Investment portfolios, credit card #s, Trusts, offshore accounts, Your Travel itineries, Your Health and medical information

04 **CORPORATE WORKERS**

Company IP, Company Trade Secrets, Contract documents, Emails, Payment information, HR data

RISKS TO YOUR BUSINESS

when this sensitive data gets compromised



DATA PRIVACY COMPLIANCE VIOLATIONS
Results in: Legal / Regulatory damage

INSIDER RISKS
Results in: $ and Reputational damage

3RD PARTY RISKS
Results in: Relationship damage

LOSS OF TRADE SECRETS, IP THEFT
Results in: Legal / Reputational Damage

RANSOMWARE, PHISHING, IDENTITY THEFT ATTACKS
Results in: Revenue Loss

IMPACT OF MISHANDLING SENSITIVE DATA

Cyberattacks on SMBs Reach Record Highs Despite Confidence in Defenses

THU | OCT 26, 2023 | 11:00 AM PDT

The 2023 ITRC Business Impact Report shows 73% of SMBs experienced a cyberattack, data breach, or both in the past 12 months. This represents a significant jump from the 58% attack rate in 2021 and 43% in 2022.

CYBERCRIME

Recruiting Firm Apparently Pays Ransom After Being Targeted by Hackers

Administrative staffing agency Career Group, Inc. this week started sending notification letters to customers who were affected by a data breach that occurred in late June.

By Ionut Arghire
September 2, 2021

Krispy Kreme is struggling to fulfill online orders after it was hit with a cyberattack

By Jordan Valinsky, CNN
1 minute read · Published 8:27 AM EST, Wed December 11, 2024

WHY SMBS DON'T INVEST IN CYBER?

LACK OF AWARENESS

Business owners typically underestimate the risks and think they are too small to suffer the consequences

LIMITED BUDGET

SMBs need to prioritize their business growth over "invisible" expenses like cybersecurity

RESOURCE SHORTAGES

Dedicated cybersecurity resources are expensive and you cannot afford them due to other competing business priorities. You may think that they may not be necessary.

MISCONCEPTION ABOUT RISK

SMBs believe they are less likely to be attacked compared to larger corporations, unaware that hackers increasingly target small businesses due to weaker defenses.

FOCUS IS ON SHORT-TERM GAINS

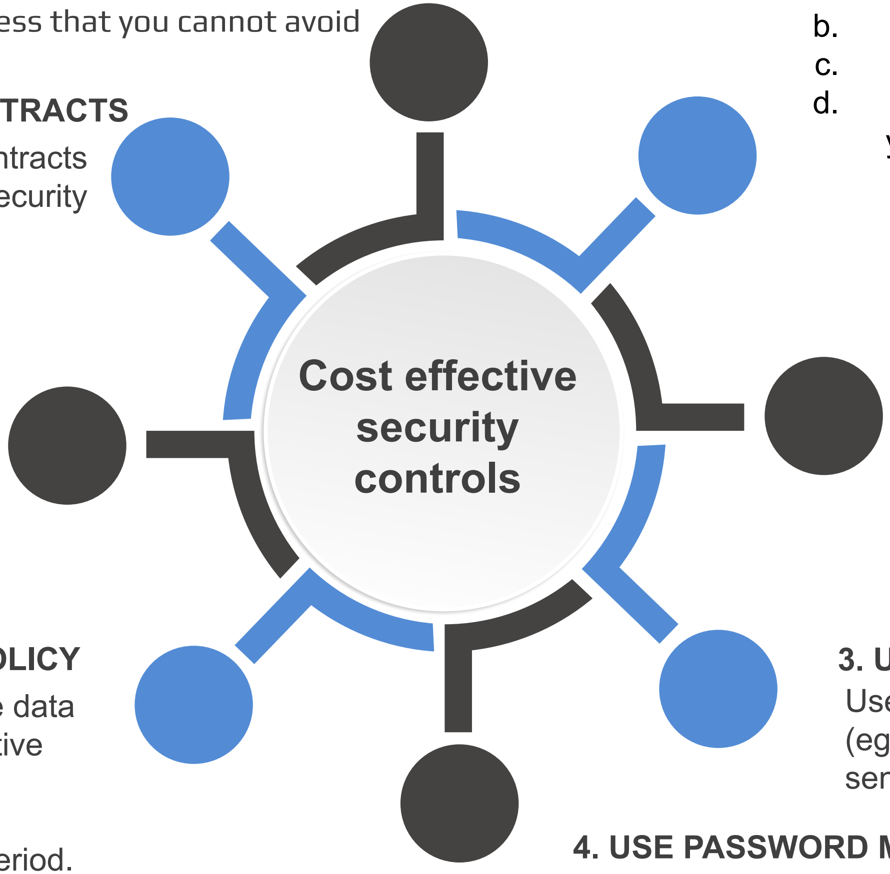
Investing in cybersecurity provides no immediate ROI, making this less appealing for SMBs focused on quick wins.

WHAT IS THE VALUE OF SENSITIVE DATA?

STOLEN DATA TYPE	ESTIMATED VALUE IN THE DEEP / DARK WEB	ADDITIONAL DETAILS
Social Security #s	$1 - $5	Cheap. Helps with identity theft
Credit / Debit card #s	$10 - $30	Value increases with higher credit limits and CVVs/PIN #s
Health records	$250 - $1000 per record	Highly valuable for Insurance fraud for the lifetime of the person defrauded
Email Login credentials	$5 - $50	Used as a gateway to steal more Personally Identifiable Information
Online Shopping account	$10 - $45	Used to access stored credit cards and access purchasing history
Corporate Login credentials	$500 - $10,000+	Price varies by org size and access level of the staff

Some Cost-Effective Solutions

Zero Cost Solutions to Businesses



1. SECURITY TRAINING

a. Make this annual mandatory
b. Prioritize on High-Risk Employees
c. Focus on what <u>NOT</u> to do
d. Log this training to demonstrate your due diligence

2. SEPARATE WORK AND PERSONAL ASPECTS

a. Harden your laptop (Antivirus, Patching, remove un-needed SW, restrict access)
b. Enable Multi-Factor Authentication
c. Disable mail forwarding
d. Change default passwords on vendor provided apps

3. USE SECURE FILE SHARING SERVICES

Use reputed cloud based secure file sharing service (eg: Box, Gdrive, Onedrive, Citrix Fileshare) to send/receive all business sensitive data

4. USE PASSWORD MANAGER TOOL

Tools like Lastpass, 1Password, Google Password Mgr reduce administrative burden on password maintenance while reducing your cyber risk

5. IMPLEMENT A DATA RETENTION POLICY

a. Policy applies to all business sensitive data
b. Identify how long your business sensitive data needs to be protected by you.
c. Create an internal policy to delete all business sensitive data beyond this period.
d. Ensure all remaining data are backed up in real-time on the cloud.

6. IMPLEMENT A SOCIAL MEDIA POLICY

a. Policy applies to everyone including high risk employees (eg: Customer facing staff, account managers, recruiters)
b. Focus on what **<u>NOT</u>** to do

7. IMPLEMENT SECURITY CLAUSE IN CONTRACTS

Minimize your liability in your business contracts something goes wrong (eg: Data breach / security incident) in your deliverables.

8. PURCHASE CYBER LIABILITY INSURANCE

Anticipate ahead and plan security incidents in your business that you cannot avoid

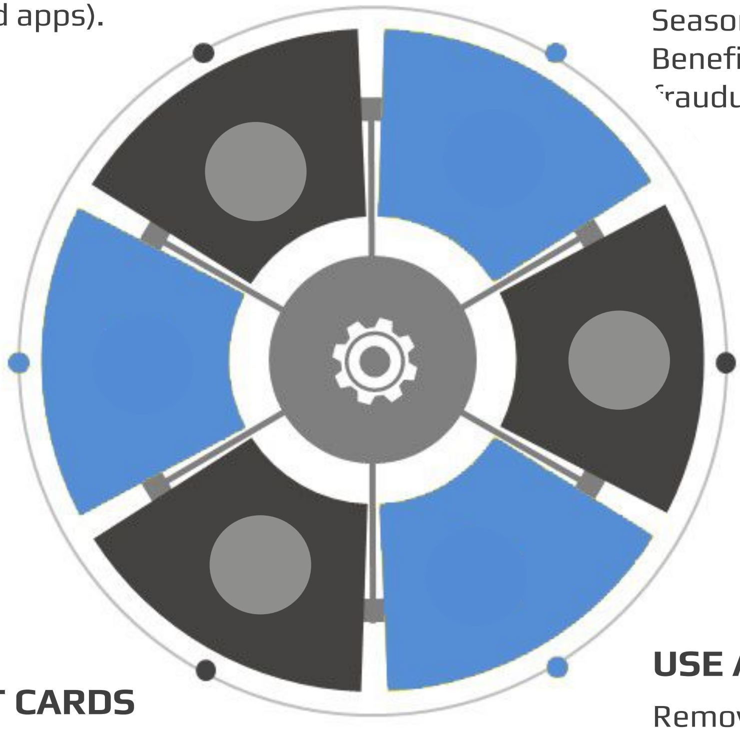
Zero Cost Solutions to Online Shoppers

ENABLE MFA

Enable Multi-Factor Authentication on all apps containing sensitive data online (eg: Health / Finance related apps).

REVIEW CREDIT CARDS / CREDIT SCORES / EOBs

Review your credit cards annually and your credit scores and social security balance statements yearly. It is a good Tax Season activity. Review your Health care Explanation of Benefits (EOBs) after every Healthcare visits to look for fraudulent charges.



USE ONLINE PASSWORD MANAGER

Do not re-use passwords. Use tools like LastPass or Google Password Manager to simplify password management. They are free and reliable!

AVOID PUBLIC WIFIS

Airport WIFIs, WIFIs operating at unknown locations are an easy target to steal information flowing through them. As a practice Do not use them!

USE A DEDICATED HARDENED LAPTOP

Remove unnecessary SW, restrict access to accounts, ensure all patches are up-to-date to harden your laptop. Use this dedicated laptop for all important online transactions

USE VIRTUAL CREDIT CARDS

Most credit card companies (eg: Citi) offer Virtual credit cards. They are randomly generated numbers that are valid for single use only.

Zero Cost Solutions to HNWIs

High Net worth Individuals

FREEZE YOUR RETIREMENT ACCOUNT

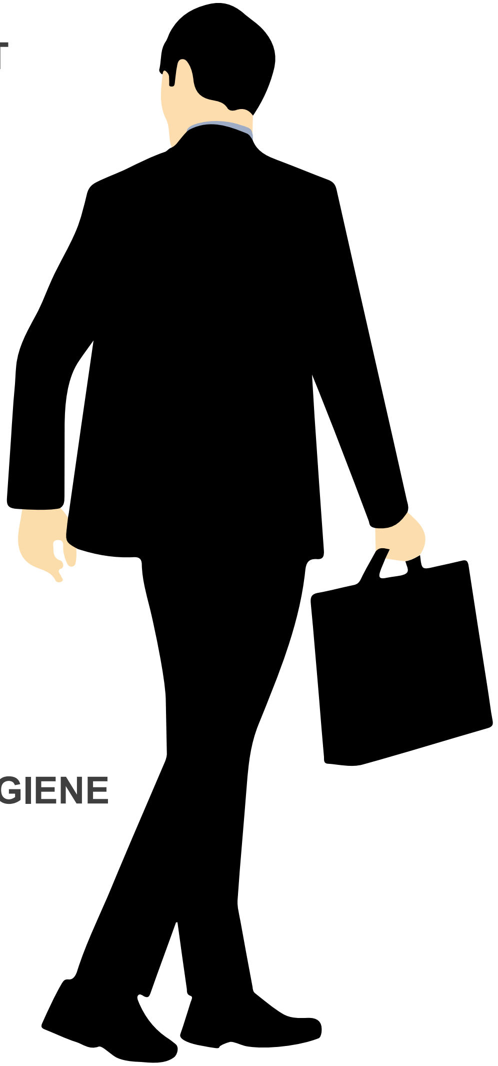
If you don't actively trade your Retirement Account, ask your provider if they can incorporate a lock (account freeze) on your account (You can unlock it when you need to) to minimize fraudulent activities.

SETUP ACCOUNT ALERTS

Create alerts on your financial accounts to alert you when transactions are done over a certain threshold and signup to be notified whenever there are changes in account settings.

EDUCATE YOUR FAMILY ON CYBER HYGIENE

This becomes important as they are in your trusted circle and could potentially be the weakest link to get to your digital assets.



MONITOR YOUR DIGITAL FOOTPRINT

Carefully evaluate what you post on social media. Your online data can be potentially used against you. Restrict who can see your posts and photos.

DO NOT CLICK ON UNKNOWN EMAIL LINKS

When in doubt, do not click on unknown links or QR codes

USE A DEDICATED HARDENED LAPTOP

Remove unnecessary SW, restrict access to accounts, ensure all patches are up-to-date to harden your laptop. Use this dedicated laptop for all important online transactions

Zero Cost Solutions to Corp workers

DO NOT MIX PERSONAL AND BUSINESS DATA

Do not use your work laptop / mobile phones for any personal use and vice versa. Everything you do on your work assets can be tracked.

DISABLE SMART VOICE ASSISTANTS

Disable voice-activated devices, such as Amazon Echo or similar smart assistants, during sensitive conversations or work activities.

USE BURNER EMAIL FOR NON-ESSENTIAL ACCOUNTS

Avoid using your primary emails for online signups. This will reduce your phishing attack surface.

EVERYTHING YOU DO ON YOUR WORK NETWORK CAN BE MONITORED

Be conscious about the files you open, the sites you visit, the search queries you execute on your company intranet. They are all attributable.

USE ONLY SANCTIONED LLMS

Use only company sanctioned AI platforms / apps to reduce accidental exfiltration of sensitive data.

LEAVE COMPANY DOCS BEHIND UPON EXIT

Assume that any document you own at work computer cannot be taken with you after you leave the company. Plan accordingly.

Emerging cyber / AI trends

Increased spend on AI

AI spend is increasing overall taking up to 15% of company budgets. It is no longer an IT tool but use cases expands into HR, Supply chain, Procurement, and Legal teams.

Time to upskill in AI

Rise in 3rd party risks

Risks from 3rd parties that you do business with can directly impact you. These risks have been on the rise and are continuing to rise.

Use contracts to protect yourself

Rise in AI powered threats

Good bots defending against bad bots are our current norm

Anticipate speed in attacks

Contact-less payment surge

Alternate payment methods such as Digital Wallet, Contactless payments, Real Time Payments, Buy Now Pay Later are on the rise.

Embrace the change!

Rise in online fraud

Online ecommerce fraud, anti-money laundering risks, and compliance / regulatory risks are rising due to AI based attacks and increased connectivity.

Be aware

Security Tips For The Holidays

Use Virtual credit cards

Use Virtual credit cards (Amex, Citi, Capital One) to pay for goods online.

Enable 2FA

Enable 2FA on WhatsApp. If you suspect your account was compromised, log off from all devices before resetting your PIN to end any active sessions using your ID.

Do not click on unknown links

Preview emails from suspicious senders to avoid opening them. Clicking links or opening PDFs can inject code into your device and notify the sender if you’ve opened the file.

Freeze unused a ccounts

If you're not actively using certain cards, enable the option to "freeze" your card temporarily via your banking app. This limits fraud attempts during downtime.

THANK YOU!

Q&A Time

Your Data is Currency. Protect it.