"Maximizing your business through the cyber security era"

Heritage Bank
Business Leaders Forum

May 16, 2019

Bob Watts
859.414.6115 x101
www.vivitec.net
BobWatts@vivitecsolutions.com

Today's Discussion

1. The Cyber Society
2. Cyber attacks and companies under 250 employees
3. How to protect your business in the cyber era

vivitec
BUSINESS SOLUTIONS

The Cyber Society

Largest and Fastest Societal Expansion in Human History

Adolescent
Evolutionary network
Virtualization
Early civil practices
Formative culture
Software is implicit
Abundant opportunities

Eradicating Limitations:
Geographic
Physical
Time
Delays
Resistance
Manual Efforts

Global Population 7.7B 2019
Internet Users: 4B+

Threats – Crime – Profiteers – National Interests – Risks - Unknowns

vivitec BUSINESS SOLUTIONS

Evolution of the Cyber Society

CyberSecurity is Essential for a Flourishing Cyber Society

Worldwide cybersecurity market at $152B in 2018 estimated at $248B by 2023. Markets and Markets, Sep 21,2018.

2.93M Cyber workforce shortage. (ISC)2, 10/18/18

Lloyd's of London estimates cyber attacks cost businesses as much as $400 billion a year.

17K+ Confirmed Data Breaches in 2018

Regulatory Fines Increasing

Ransomware - $1.5B **Industry**

Class action PII lawsuits

Enterprise & Gov't Breaches

Small Businesses now Heavily Targeted

Cyber insurance market was $4.52B in 2017 and forecasted at $17.55B in 2023. Reuters, 5/6/19

Cyber Attacks and Your Business

I'm too small and have nothing they want…

Good luck to you, I recommend updating your resume

- The largest growth area for targeted cyber attacks in 2018 was businesses with fewer than 250 employees
- The majority of cybercriminal activity is indiscriminate
- Only 33% of all attacks were considered "targeted"
- 43% of all breaches (aka data or money loss) involved small business victims
- Organized cyber criminals target vulnerable computer systems regardless of the company
- While financial and retail companies continue to be targeted the most, criminal activity in 2018 spans across all industries
- All businesses, regardless of size, are at risk

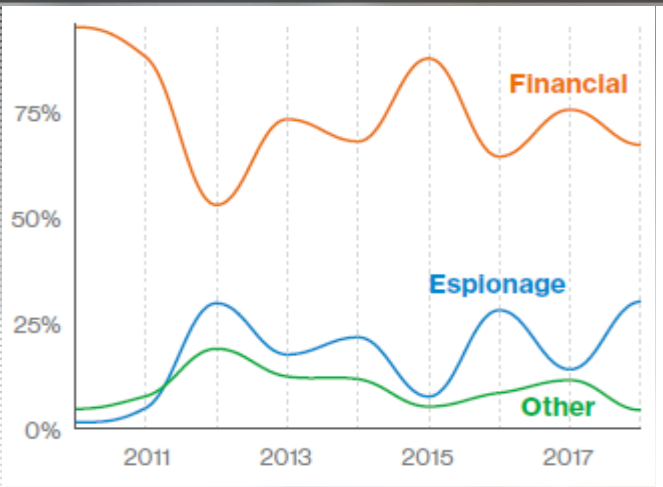
Good News…You Don't Have to Invest Like GE Aviation to Protect Your Business

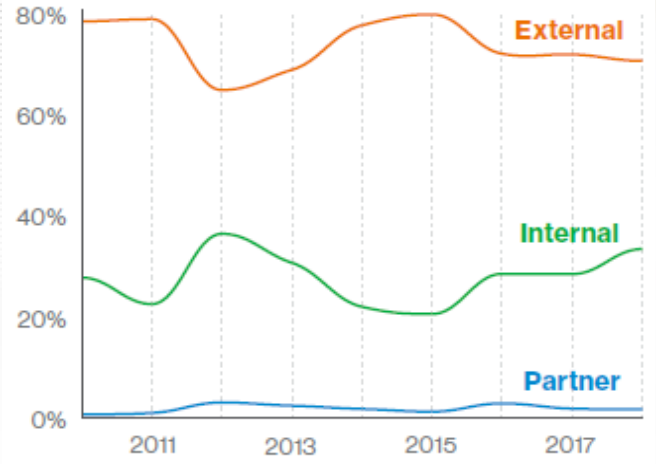
Business Leaders/Owners Should Know

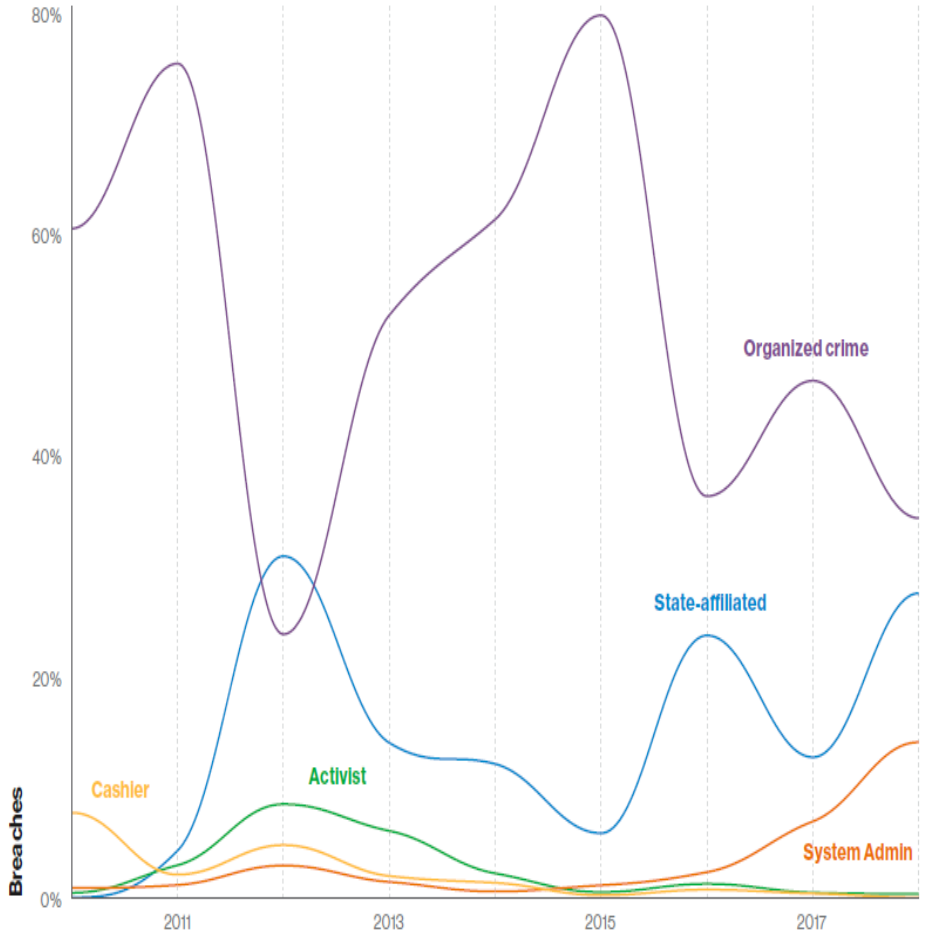
Leaders / Owners
You must
engage, inquire,
make decisions,
and own the
security plan.

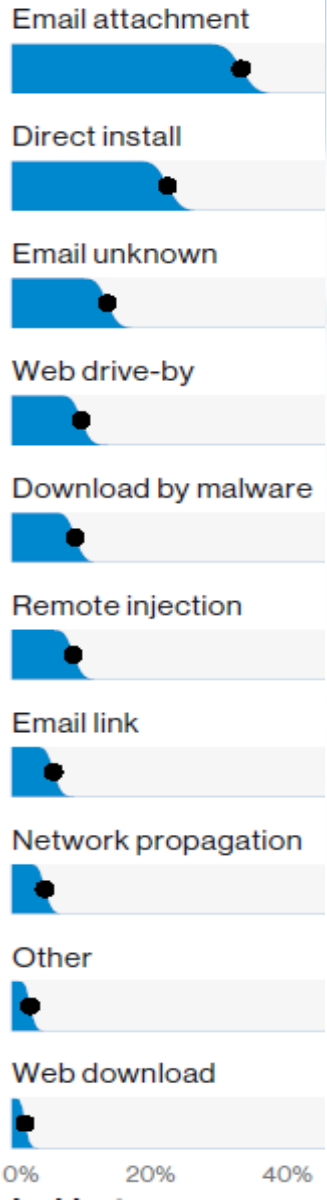
- Businesses can pursue maximum technology gains while managing increased risks and protecting our brand, business, and assets.
- Management of technology, cyber security, and ramifications are owner and board level responsibilities and expectations today.
- Determining where to focus, how much to invest, and tailoring your technology and cyber plans for your business is a new, required, business management skill.
- Minimizing business, real-life, damages permeating out of cyber society incidents may define your reputation, brand, longevity, and growth even more than your products and services.
- Cyber security defense is a skill set that involves IT and Tech but is specialized and a very different competency. Your “Tech Guy” is typically not prepared, skilled, or an expert in protecting your business. Look beyond the marketing.

Attacks – Why, Who, How, What









Spear Phishing

Sextortion

Ransomware

CEO Fraud

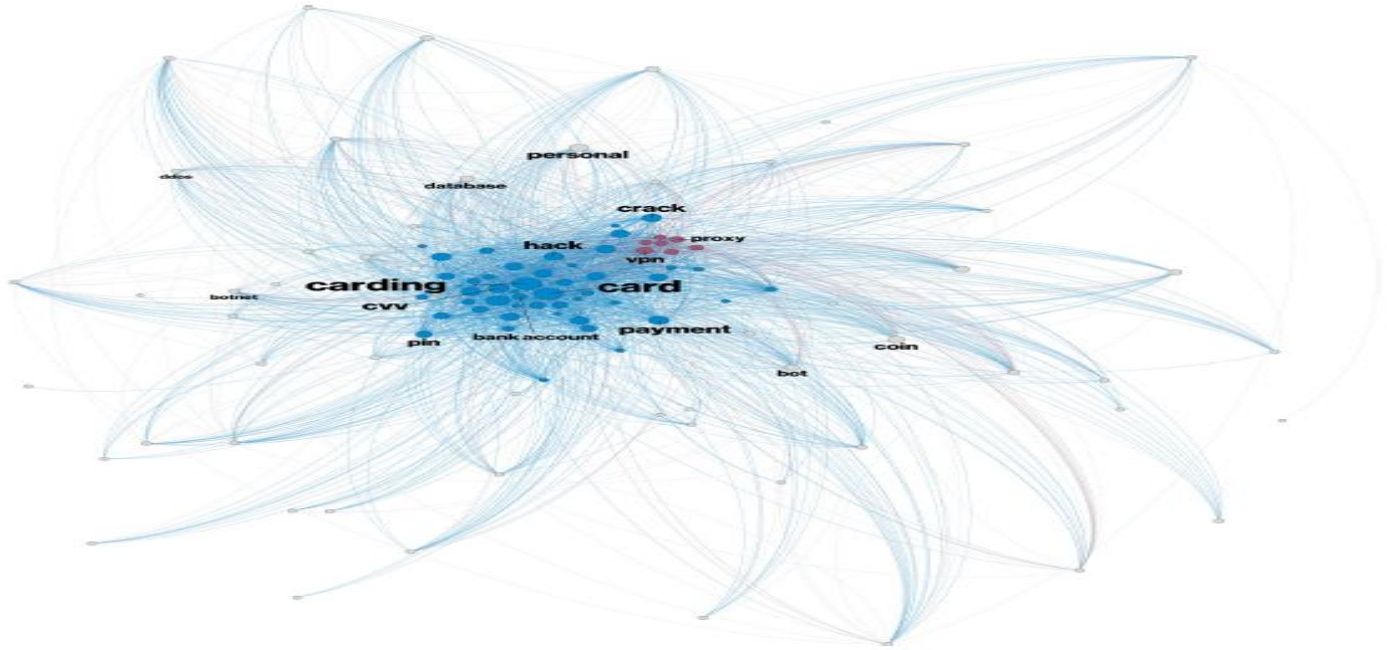
Credential Compromises (email)

Account Access

The Dark Web

The cyber black market (aka Dark Web) is a sophisticated, online, evolving market where criminal cyber products and services are sold and exchanged.

Hacker service	Price
Visa or MasterCard credentials	$7
Credit card with magnetic stripe or chip data	$15
Premium American Express, Discover Card, MasterCard or Visa with strip or chip data	$30
Bank account credentials (balance of $15,000)	$500
Bank account credentials (balance of $70,000 to $150,000)	6% of account balance
Large U.S. airline points accounts	1.5 million points cost $450
Large international hotel chain points account	1 million points cost $200



Are your business email credentials for sale?

vivitec BUSINESS SOLUTIONS

Cyber Security Business Plan

1. Identify Business Valuables and Risks
2. Document Simple Security Plan
3. Implement Technology Defense
4. Train Employees
5. Check 3rd Party's Security
6. Evaluate Security Monitoring & Testing
7. Rehearse Response Plan
8. Validate Backup and Recovery
9. Purchase Cyber Insurance

OK,
Who wants to improve their cyber security and beat these criminals?

Plan Framework
Identify
Protect
Detect
Respond
Recover
NIST Based

What really annoys me about security talks…

Know What You Are Protecting

1. Identify Business Valuables and Risks

Focus on your business…not everything you've ever read about cyber security threats

- What are your "Business Valuables"?
  - Personal / Client Information (PII, PHI, CHD)
  - Access and Privilege to Move Money
  - Computer Assets that Run the Business
  - Stored data, Intellectual Property
- Where are they located and how do they get there?
- What are your risks?

2. Document Simple Security Plan

This is about confidence with customers and the knowledge that you are working to maximize your business

Document a simple plan (outline)

- Describe your assets and risks from step 1.
- Describe how you protect business valuables
- Describe any security awareness training you've planned
- List anything you are using to detect a security incident
- Bulletize the steps you'll take if you suspect a breach or incident
- Create a call list of who you'll call for incident help
- Describe how you will recover your systems post incident
- Review and work the plan a few times a year as you begin

Decide how much help or investment you'll make based on amount of business risk you've identified and the level of plan that seems reasonable.

Fortify

3. Implement Technology Defense

Don't get overwhelmed…

Focus on key areas…

Do the basics consistently…

Maintain what you've committed to do…

Initially focus on protection related to your business valuables

- Managed defense software (AV/AS/MW) on all computers
  - Business grade (not "free"), on, updated, same version, US based, and maintained. Centralized management and validation is better.
- Managed patching process
  - Updates with Validation – Operating Systems and Security Patches main focus
  - Make determination on automated application patching (e.g. Browsers, etc)
- Managed Network Domain with Rules
  - All computers connected to common domain
  - Security policies configured and enforced
- Passwords
  - Enforce complex passwords, 8 digits+, and unique to each system
  - Leverage password managers
  - Everyone has unique login
- Business Equipment (PC's, Network)
  - Use business grade devices and software – keep your business out of Best Buy
- Next Generation Computer Defense (MDR)
  - Behavioral rules, vs signature ID, plus automated actions
  - Now priced for all businesses based on computers per month with 24x7 SOC
- Electronic Information
  - Encryption (while stored and moving)
  - Don't forget backup data, hosted data, 3rd parties
  - Don't forget email, scan/printers

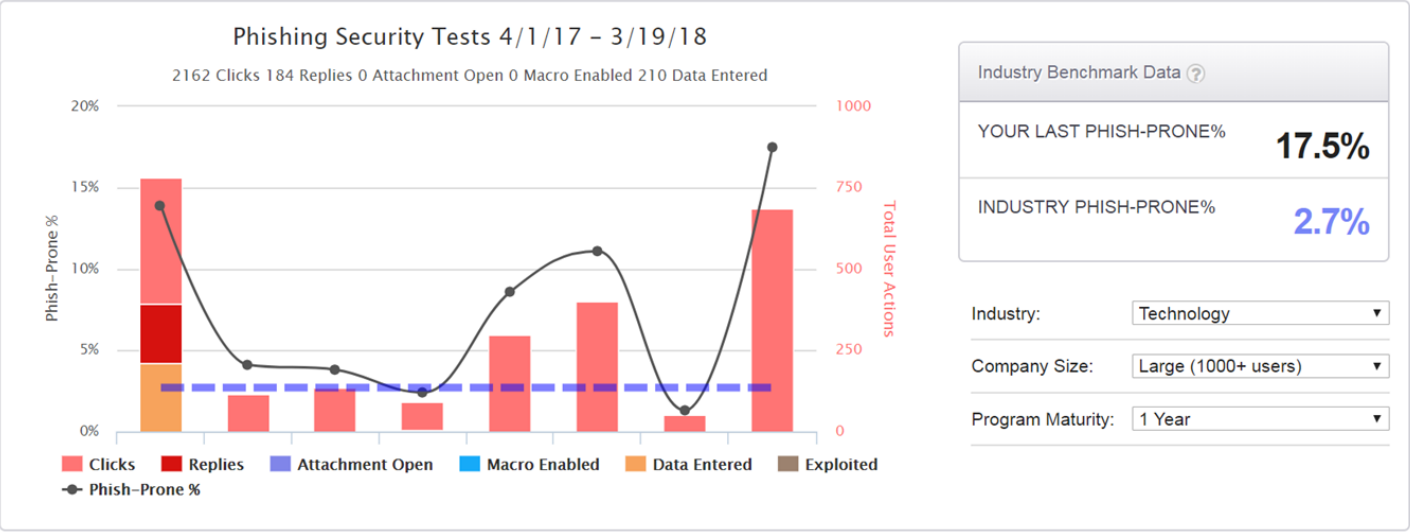
"IT security vs IT guys"

Invest in the "Weakest Link"

4. Train Employees

- Training should be short, interesting, and effective
- Focus on what will protect your valuables
- For most businesses, priority should be on:
  - #1: email and phishing
  - #2: passwords and password management
  - #3: social engineering
- *And – Test Everyone!*

Healthy Paranoia is good for business!



Man the Foxhole

5. Check 3rd Party's Security

Trust but Verify!

- Focus on parties working with or access to business valuables
- Verify their security of the services you utilize
- Request any testing or certifications they perform
- Review their personnel policies for their employees or contractors working for you

6. Evaluate Security Monitoring & Testing

Who's watching, testing and responding?

- Quick detection of an incident with action is crucial
- SOC – 24x7 security professionals responding to alerts
  - MDR – immediate notice and action – available and affordable
  - SIEM working on critical technology areas related to business valuables. (Email, Firewall, Main Servers, Network Devices, etc)
- Ongoing vulnerability testing (Int/Ext) – semi-annually+
- Get a quote, align services with business valuables and risks, and make an informed decision

It Happened…Now What?

7. Rehearse Response Plan

Critical to protecting your company's brand.

- Do some quick "G oogle" research on response plans
- Engage business leaders and write down what you would do if you suspected a breach
  - Who should employees notify
  - What do they do at their PC (e.g. PC - leave it running, disconnect it from internet)
  - Who gets notified next
  - How do you get together or meet
  - Who's in the team that will investigate and resolve the incident
  - Do you have industry, contractual, or legal requirements (e.g. notification, etc)
  - What's the communication plan for employees, customers, law enforcement, others
- Do a "table top" walk through of the plan with key employees
- Improve the plan over time

8. Validate Backup & Recovery

What's your recovery time…are you sure?

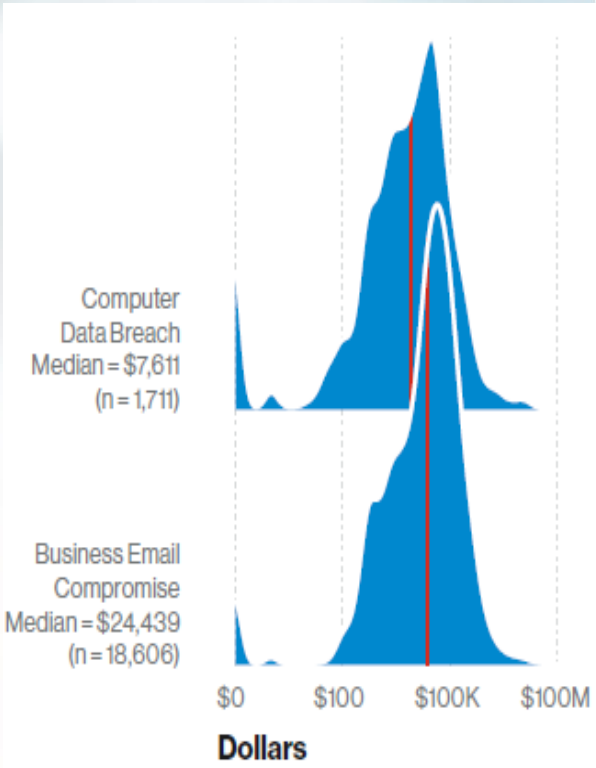
- Decide how long you can be "down"…what's the $ impact of an hour / day / week without your server, apps, PC's, etc.
- Backup Levels:
  - High Availability – No User notice operational recovery – Most expensive
  - Backup Disaster Recovery – 1-3 hours operational recovery
  - File Based Backup – 2 business weeks operational recovery – Least expensive
- Must do:
  - Periodically validate that you have a good backup that can be used
  - Backups monitored daily
  - Automated
  - Data encrypted in storage and transit
  - One copy in a different network (e.g. cloud, segmented network)

Insure the Risk $

9. Purchase Cyber Insurance

Align insurance with business impact in $ from breach, fines, recovery costs

- Policies have matured enough for general business consumption
- Keys to insurance:
  - Review and Understand Exceptions
  - Understand Insurance "requirements" and maintain them
  - Align coverage with typical incidents for your business.
    - Incident Response Costs
      - (Forensics, Public relations, Purchasing "Identity protection, n for clients", New technology, Legal fees, Business impact during incident, Subsequent business impact/losses)
    - Amount "stolen" from breach relative to your business



Vivitec officially adopted a position in 2018 supporting Cyber Insurance for every business that relies on technology as long as the policy is thoroughly vetted for exceptions, requirements, and reasonable pricing.

Northern Kentucky Businesses

Ensure Your Cyber Security Plan & Technology is Industry Compliant, Personalized for your Business, and Maintained

Thrive in this evolving cyber society…

Key Elements:

1. Identify Business Valuables and Risks
2. Document Simple Security Plan
3. Implement Technology Defense
4. Train Employees
5. Check 3rd Party's Security
6. Evaluate Security Monitoring & Testing
7. Rehearse Response Plan
8. Validate Backup and Recovery
9. Purchase Cyber Insurance

Promote Your Cyber Security Efforts

Customers are taking notice of how businesses secure their data and are more willing to trust and reward businesses for good security practices. With cybercriminals now targeting businesses of all sizes and types, it's an opportunity to market and promote that your business is serious about cyber security and protecting their information.

Questions / Discussion

As a Northern Kentucky based firm bringing global experience in Technology, Service, and Cyber Security to market, Vivitec is honored to be granted the privilege of serving our clients and this community.

We Believe

Technology should be simple, secure and reliable
Business can and should be accelerated by Technology
Protecting business assets from cyber threats is attainable
Client service is built on great partnership experiences

Our Approach

Understand our client's business and their technology
Leverage our years of experience and strategic partnerships
Provide services that add value to our client's
Focus on preventing issues before they impact business
Become a trusted business technology guide

Bob Watts
859.414.6115 x101
BobWatts@vivitecsolutions.com
www.vivitec.net

Thank you!

References

- Wikipedia, January 2019, population statistics
- InternetLiveStats.com and InternetWorldStats.com, 1/19
- Global WebIndex
- StatCounter.com
- Akamai's State of the Internet Report
- GSMA Intelligence
- Global Data Intelligence
- Ericsson Mobility Report
- Verizon DBIR, 2019
- Market and Markets, 2019
- E&Y, Cybersecurity and the Internet of Things
- STC Small Business Analysis
- Trustwave 2019
- NIST CSF
- TechPro Research