VESTIGE
Digital Investigations

CyberSecurity for SMBs

TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™

Northern Medina County Chamber Alliance

Brunswick, Ohio

January 18, 2017

Today's Cyber Landscape

- You read the headlines
- You see the statistics

You're left wondering…

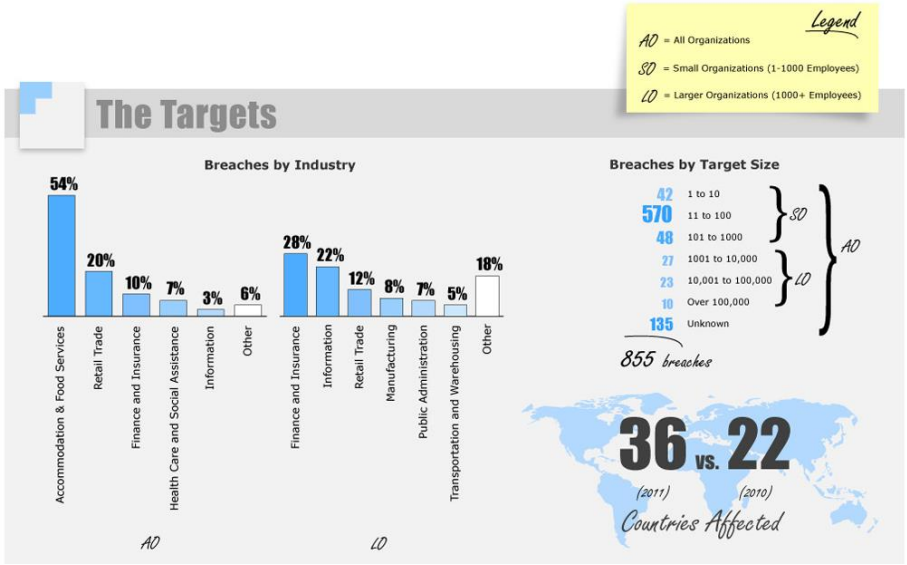
- Is it REALLY that bad?
- What's ACTUALLY going on out there?
- How can MY organization be a target?

Today's Cyber Landscape

What's it look like out there?

By the Numbers

- 63,000+ **reported** security incidents annually
- Over 822 million records compromised
- Average cost to organizations with 1000+ employees is $7.7m
- The US Military Treats Cyber as one of five domains: air, sea, land, space and now cyber.-General Michael Hayden. Former Director CIA and NSA



Some more scary thoughts

- Cybercrime costs in US up 19%
- Average cost of compromise - $3.4 million
- 66% of companies say it is likely or very likely they will experience an Advanced Persistent Threat (APT)… and
- 1 in 3 of those companies say they're not prepared


Cybersecurity
Skills Crisis
Too Many
Threats
62% INCREASE IN BREACHES IN 2013[1]
1 IN 5 ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK[4]
US $3 TRILLION TOTAL GLOBAL IMPACT OF CYBERCRIME[3]
7½ MONTHS IS THE AVERAGE TIME AN ADVANCED THREAT GOES UNNOTICED ON VICTIM'S NETWORK[2]
2.5 BILLION EXPOSED RECORDS AS A RESULT OF A DATA BREACH IN THE PAST 5 YEARS[5]
Too Few
Professionals
62% OF ORGANIZATIONS HAVE NOT INCREASED SECURITY TRAINING IN 2014[6]
1 OUT OF 3 SECURITY PROS ARE NOT FAMILIAR WITH ADVANCED PERSISTENT THREATS[7]
<2.4% GRADUATING STUDENTS HOLD COMPUTER SCIENCE DEGREES[8]
1 MILLION UNFILLED SECURITY JOBS WORLDWIDE[9]
83% OF ENTERPRISES CURRENTLY LACK THE RIGHT SKILLS AND HUMAN RESOURCES TO PROTECT THEIR IT ASSETS[10]
Enterprises are under siege from a rising volume of cyberattacks.
At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.
SOURCES: 1. 2014 Internet Security Threat Report, Volume 19, Symantec, April 2014; 2. M-Trends 2014: Attack the Security Gap, Mandiant, April 2014; 3. Increased Cyber Security Can Save Global Economy Trillions, McKinsey/World Economic Forum, January 2014; 4. ISACA's 2014 APT Study, ISACA, April 2014; 5. An Executive's Guide to 2013 Data Breach Trends, Risk Based Security/Open Security Foundation, February 2014; 6. ISACA's 2014 APT Study, ISACA, April 2014; 7. ISACA's 2014 APT Study, ISACA, April 2014; 8. Code.org, February 2014; 9. 2014 Cisco Annual Security Report, Cisco, January 2014; 10. Cybersecurity Skills Haves and Have Nots, ESG, March 2014
CSX CYBERSECURITY NEXUS
ISACA Trust in, and value from, information systems
MAY 2014

Why Should we care?

- C-Suite / Business Executive / Leadership Team misconceptions

From their perspective

- The organization has a firewall protecting them from OUTSIDER threats?

From their perspective

- The IT Department/Company/Parent Company handles their CyberSecurity?

From their perspective

- They are (fill in the blank) compliant…CyberSecurity is just not an issue…

From their perspective

- They (believe they) don't have anything sensitive that anyone would want?

This stuff doesn't apply to you, right?

- The Difference between Your Organization & Everyone Else…
  - You don't have financial info that someone would want
  - You don't have intellectual property of interest
  - No state secrets or geo-political information
  - Not enough records to warrant concern

So why should you care?

Case Studies

ALL of the following had:

- A firewall
- An IT Department/Company handling their CyberSecurity
- Didn't have anything they believed to be of value
- And were compliant with all regulations and compliancy requirements

Case Studies

- Down on the Pharm:
  The case of the digital bank heist
- Knock, knock…FBI who?
- A bad day in the IT Department
- Teach a Man to Phish: Business E-mail Compromises
- A bad day in the HR Department

It’s not safe to turn on your computer.

From Our Perspective

- We are Electronic Evidence Experts
- Specialize in: Digital Forensics & CyberSecurity
  - 18 Years in CyberSecurity realm
  - 16 Years in Digital Forensics
  - Incident Response / Data Breach is a large percent of what we do.

We are parachuted in to organizations to solve problems

Experts at Applying our Knowledge

- Closed-circuit
  - What we find “in the wild” helps us to help you be more secure.

So what's really going on out there

Top Ten Threats

1. Social Networks
2. Third Party Attacks
3. Internet of Things
4. Reputational Damage
5. Targeted Botnets
6. Data Privacy in the Cloud / Big Data
7. Advanced Persistent Threat (APT) /Cyber Warfare
8. Mobile Applications/BYOD
9. Phishing
10. Skills Gap / Routine Maintenance Neglected

Social Networks

- **Personally Identifiable Information**
  - **"Twenty Questions"**
    - What was your most embarrassing moment?
    - Have I ever played hooky?
    - What was the name of my first elementary school?
    - What was my favorite pet's name?
- **Disclosure of whereabouts**
  - "Looking forward to the family vacation next week at Disney World."
- **Malware, Spyware**
- **Hoaxes**
- **Disclosure of Secrets**
  - "Rumor has it the Acme Widgets acquisition fell through"
  - Working to troubleshoot a major software bug we just found"

Third Party Attacks

- Trusted Connections
- Upstream/Downstream Liability
- Shared Data, Shared Infrastructure
- Employees – VPN

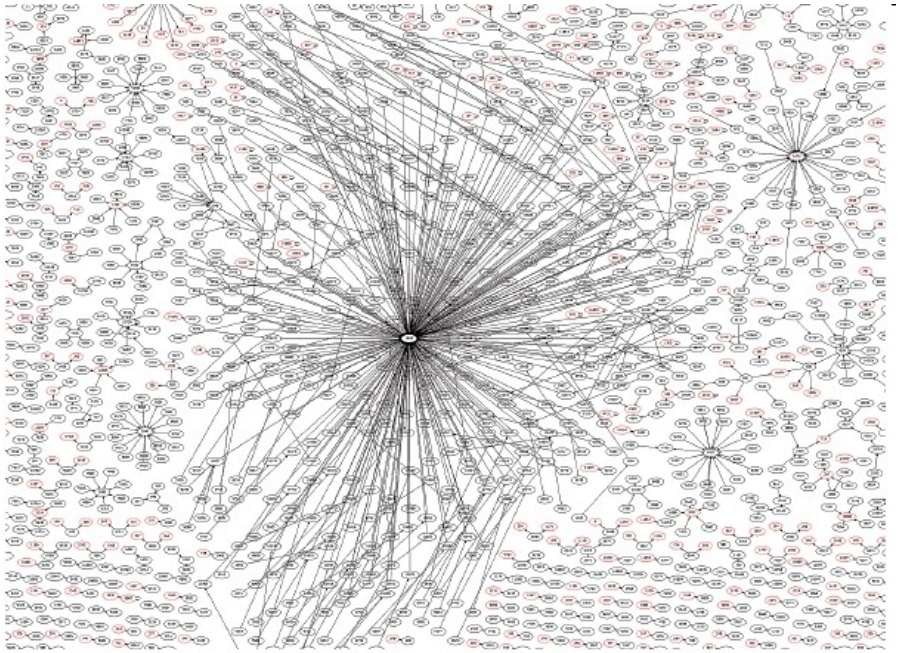


Image 1: Malware Delivery Networks and Their Correlated Web Sites

IoT: Insecurity of Things

- Ubiquity of Interconnected Devices
  - Designers not attentive to security needs
  - Novel uses of technology without forethought
  - Lack of standards
- Integrated with back-end systems

Targeted Botnets

- Thousands to Tens of Thousands of “drones” under control of attacker
- Wide Destruction
- Migration
  - Used to be: General targeting
  - Now: Targeted
    - DDOS – More advanced (Adaptive)
    - Malware Delivery
    - Spam

Cloud Computing

- Tempting Target
  - Personal information
  - Passwords
  - Trusted “gateway” to other resources
  - APIs with vulnerabilities
  - “Mother-lode” for the successful attacker
  - Big Data = Big Target!

Advanced Persistent Threat (APT)

- You have something attacker wants:
  - Intellectual Property
  - Cash / Financial resource stream
  - E-mail addresses
  - Employee's names
  - Project names & participants
  - Back-door connectivity (trusted) to intended target
- Concerns:
  - Downstream liability
  - Upstream liability (3rd Party Liability)
  - Getting them the hell out of there

Cyber Warfare

- Specific, State-sponsored attacks
  - Intellectual Property
  - Financial Market/Resources
  - Back-end to Trusted Source

BYOD: Bring Your Own Disaster

- Ubiquitous
- Sheer Power = Expanded Use
- Connectivity & Integration
- BYOx
  - Access to IP
  - Ability to bypass corporate safeguards
- Easily lost/stolen
  - Out-of-control of owner/user

Phishing

- Plays on un-aware victims
- Getting harder to tell real from fake
- Spear-Phishing

Skills Gap /Maintenance Negligence

- Inability to find, hire & retain qualified individuals
  - Not identifying the “right” things to secure
  - Not monitoring/looking at things consistently
  - Too much to accomplish with too little resources
  - Failure to put Best Practices in place
  - Failure to properly maintain (on a consistent basis)
    - Failure to update security patches
    - Sunset versions
    - Passwords not expiring
    - Service accounts (especially default)
    - Elevated accounts for installed software/outsourced arrangements
    - Accounts not disabled
    - Poor Passwords

How You Become a target

- Crime of Opportunity
- Collateral Damage
- Part of an Unlucky “targeted” Group
- Purposefully Targeted
- Evolved & Evolving Landscape

Crime of Opportunity

Collateral Damage

- Someone else's system gets compromised
- Someone else's e-mail gets compromised
- Employee/Owner's credentials is compromised

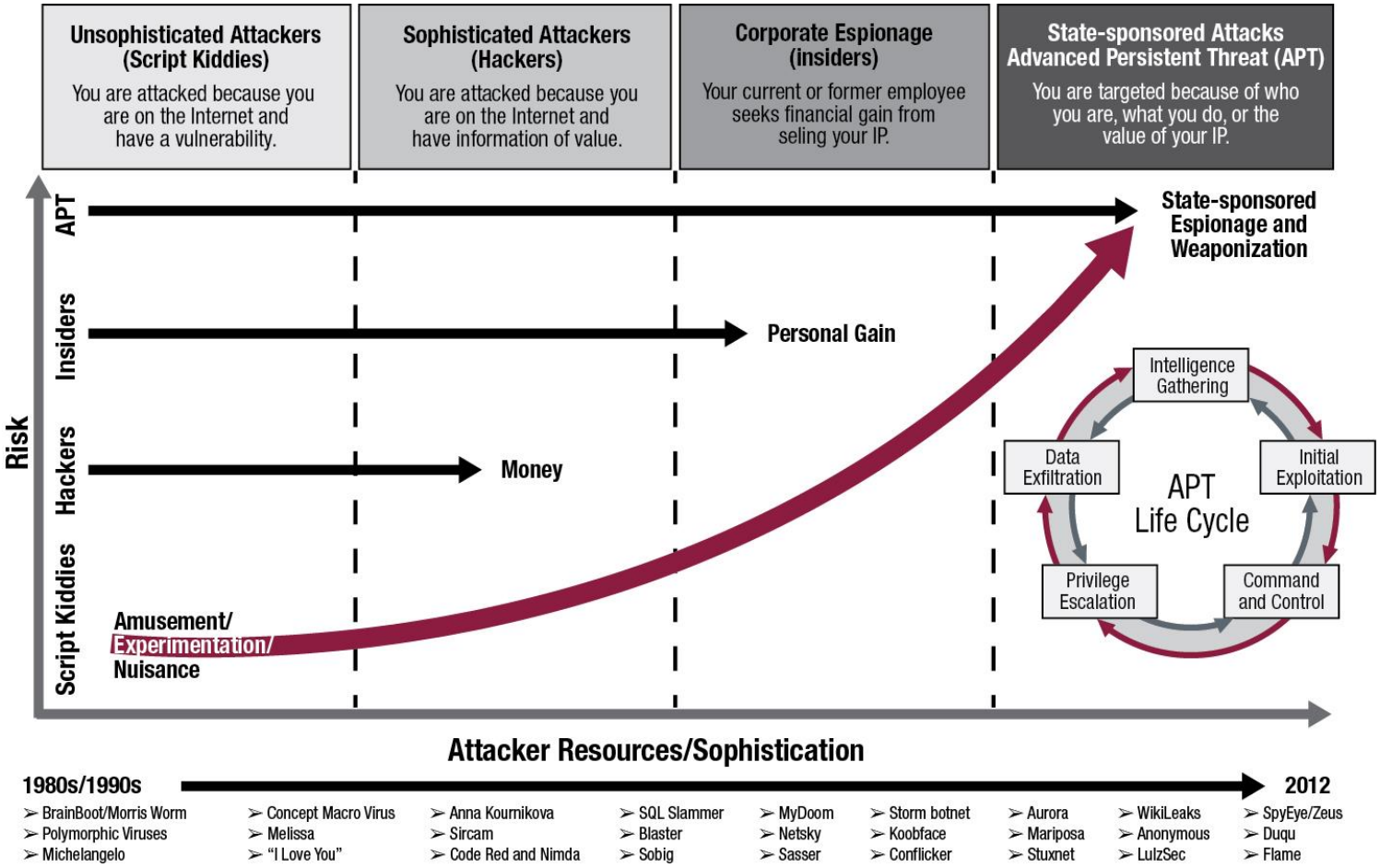
Part of an Unlucky "targeted" Group

- Wrong place…wrong time
- Examples:
  - Retail
  - Financial Service
  - Professional Services
  - Manufacturing
  - "Group du jour"

Purposefully Targeted

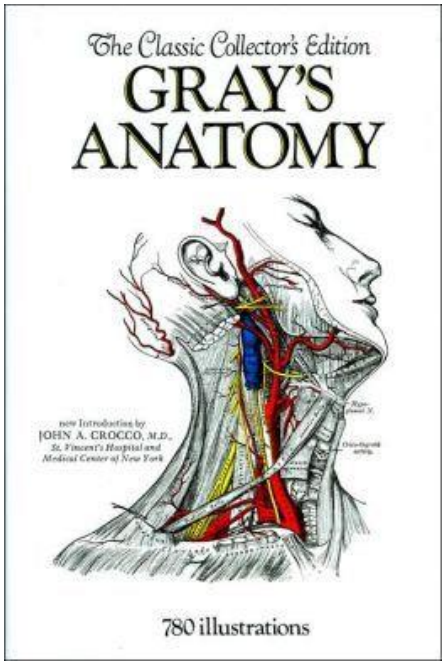
- Previous Victim
- Intellectual Property
- “Jumping Off” Point

Evolved, and Evolving Landscape



Anatomy of a Breach

How the Bad Guys Get In, Stay In and Do Damage



The Impact

- Before we understand what…we need to understand why!

The Impact: Financial

- Costs
  - Lost productivity
  - Lost time & wages for those directly impacted
  - Investigative professionals
  - Legal advisory fees
  - Remediation
  - Notification
  - Customer/Employee Assistance (Call Center)
  - Credit Monitoring
  - Loss of Business
  - Public Relations
  - Litigation
  - Penalties

The Impact: Reputational

- Loss of Revenue surrounding Customer Confidence
- How were stakeholders handled
- Sharesholders & other stakeholders

The Impact: Legal

- Breach Notification Laws
- Regulatory Compliance – Penalties & new hoops
- Downstream Liability
- Shareholder/Stakeholder Litigation

The Impact: Re-Victimization

- Soft Target for future
  - Black Market sale of your infrastructure info & “what worked”
- Did you get everything cleaned up in the first place?

Targeting

Recon

Compromise

Persistence

Exfiltration

The Big Issues

- Average Time Intruder is in System:
  - 9 – 15 months
- Average Visibility:
  - 3 – 4 months
- 95% of time discovered by an external party

The Big Issues

- Knee-Jerk Reaction:
  - "Get them out of our systems…NOW!"
- No Consideration for:
  - The C-Suite's Big 4
    - How do we know we got everything?
    - How bad was the compromise, really?
    - What got compromised, specifically?
    - What are our notification obligations?

The Big Issues

- Misbelief that CyberSecurity can be solved with:
  - Money
  - Technology

- Those things help…but it's much bigger than that!

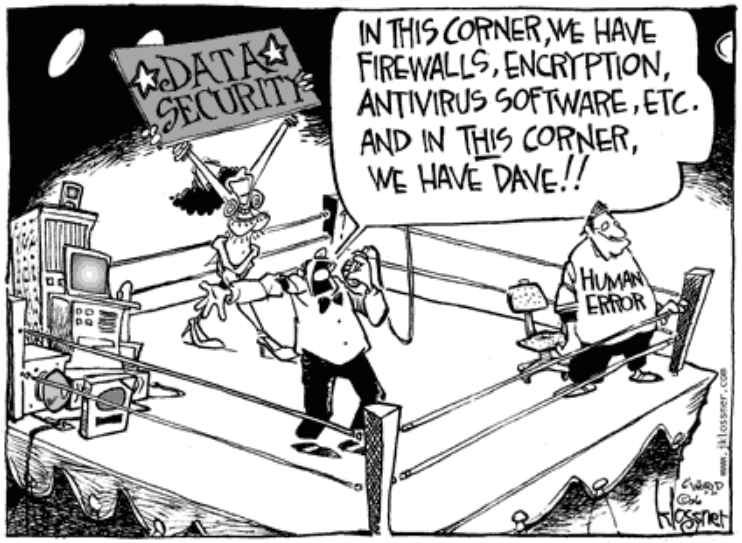
The Big Issues

- Misbelief CyberSecurity is a once-and-done proposition

- Did I mention the bad guys are Evolved AND Evolving?

The Big Issues

- IT Security is NOT an IT Problem
  - "It's the Users… Stupid !"



Why is IT Security so Hard?

- IT Security is not solely an IT Problem
  - Users
  - Convenience-Security Balance
  - Training / Focus
    - What is IT put into place to do?

Protecting Yourself

What You Can Do…Starting Today

A 9 Step Program

- Change in Attitude
- Recognize Impacts of Not Being Secure
- “It Ain’t Easy”
- Commit to Being Vigilant
- Establish a CyberSecurity Program
- Hold People Accountable for CyberSecurity
- Educate
- Provide Resources for CyberSecurity
- Plan for the Inevitable

Change in Attitude

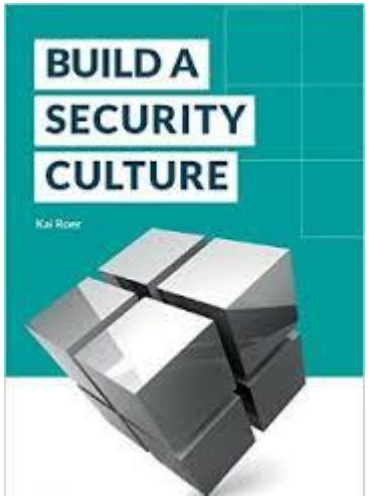
- You MUST accept that you're a target…just because
  - Always-on connectivity
  - Opportunistic
  - You DO have SOMETHING that SOMEONE wants

The Price of Not Being Secure

- Hard Costs
  - Remediation
  - Investigation
  - Notification, Credit Monitoring & Call Center
  - Litigation & Penalties
- Soft Costs
  - Lost Productivity, time & wages for those involved
  - Loss of Business
  - Public Relations

"It ain't easy"

- Give up on the belief that CyberSecurity is easy and can be solved with **money** and is a **one-time initiative**.
  - Most of the changes come down to:
    - Configuration
    - Attitude – being vigilant
    - Paying attention
  - Achieve a "culture of security"



Commit to Becoming Vigilant

- "Always On" means you need to become "Always Aware"
  - Question the out-of-the-ordinary
    - Ex. Log File Review of incident
  - Build new habits out of old
    - Ex. Review of e-mails for phishing attempts

Establish a CyberSecurity Program

- Understand your risks and prioritize them
- Assess/Audit your environment regularly
  - Understand your options:
    - DIY vs External – Biases?
    - Types – Vulnerability Scanning, Penetration Testing, Ethical Hacking, A&P, White-hat/Grey-hat hacking
- Layered approach & focus on external and internal
- Prioritize the results
- Remediate the issues

Hold People Accountable

- CyberSecurity isn't an IT issue – it's everyone's issue
- Make sure everyone understands their part in the picture; hold them accountable for action & inaction
- Establish policies
- Ensure compliance

Educate

- People “don’t know what they don’t know”
- Need to sensitize them to what’s out there

Provide Resources for CyberSecurity

- Resources need to be made available:
  - Tone at the Top
  - Time to research and remediate
  - Some money
- Don't fall into trap of believing "money solves everything"
- Don't believe vendor's claims that their "product" is the panacea.

Plan for the Inevitable

- The 6 Ps
- During an Incident is the WORST time to plan
- Need to know what steps to take
- Create an:
  - Incident Response/Data Breach Plan
  - Up-front (Now is a great time)

Q&A

Greg Kelley, EnCE, DFCP

Vestige Digital Investigations

Cleveland | Columbus | Pittsburgh
330.721.1205
gkelley@vestigeltd.com
www.vestigeltd.com