Nyse & Knotty

A story of Unfortunate Coincidences, Poor Planning and Worse Execution

Chapter 1

The Ethical and Legal Framework for Discussion

- Ethical Obligation
  - Competence means understanding technology
  - Competence means understanding how to secure information in your possession
  - Ethical Obligation to Preserve Confidentiality
  - Ethical Obligation to Protect Client Funds
- Legal Obligation
  - From the AG's Office – failure to maintain a basic level of information security may be a violation of Consumer Fraud law
  - From the AG's Office – Requirements for breach notification and resolution
- Practical Obligation
  - Do you want to be the headline on the 11:00 o'clock news

Cloud Computing Issues

- No Prohibition on using cloud based resources
- Rules of diligence and competence apply
  - Stability and reliability of provider
  - Security services provided and reputation of the provider
  - Access to information by service provider personnel
  - Assurances regarding confidentiality
  - Termination of Service – Access to data, options to insure service does not retain data
  - Available resources for document retention
- Example – SpiderOak vs other file management services

Management of Information Technology Systems

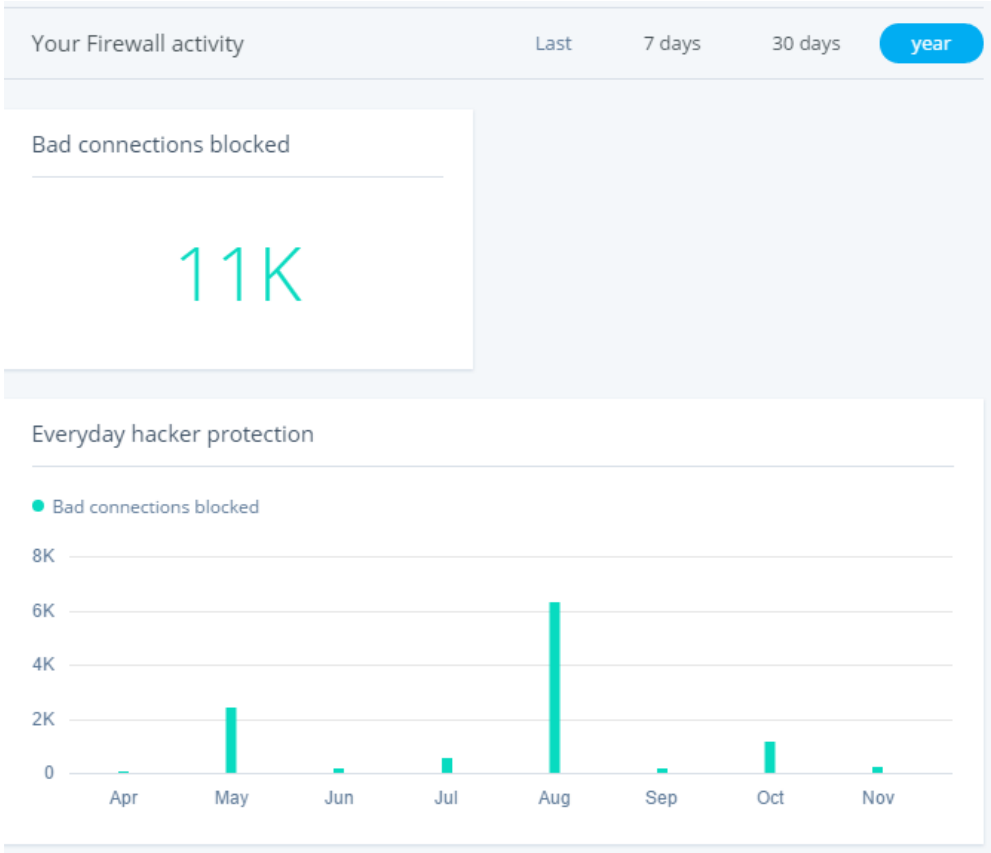
- Do not use out of date software or operating systems
  - Available exploits and defects are well known
- Apply all current patches to software, operating systems, smartphones, servers
  - General advantage to cloud based systems – someone else responsible for patching
- Be aware of issues with hardware and software
  - Windows and Apple OS X versions expire and developers stop patching systems

Internet Access and Networking

- WIFI connections, internal or external are inherently suspect
  - Tools to monitor WIFI connections are easily obtainable at little or no cost
  - Antennas for long range snooping are cheap
  - Tools to crack WIFI passwords and access are free and easily available
- Public and quasi-public WIFI hotspots are targets for people with bad intentions
- Avoid public WIFI hotspots
- Use Personal Hotspots (MiFi or cell phone hotspot) instead of public hotspot
- USE Virtual Private Network (VPN) to connect over any non-secure connection
- Use only secure internet protocols (https) for web access

Are You Under Attack

- YES!!!!
- Two weeks of activity using public WIFI in August
- No office is too small –
  - Automated attacks
  - Take advantage of any breach



Chapter 2

The Classic Email Compromise

- A system is hacked
  - Attorney or client
- Bad Actors monitor the email for signs of a transaction
- Email redirecting funds are sent
  - Maybe from a legitimate account (Nyse's account hacked)
  - Maybe from a spoofed account (Client account hacked)
- Warning signs
  - Urgency
  - Request out of character
  - Redirection of Communications

Antidotes

- Limit access to accounts to those that need access
- Written protocol for transfer of funds (internal and external)
  - Two persons, one a principal to authenticate transfer
  - Protocol with bank
  - No deviations from protocol
- Written protocol for confirming with client
  - No changes in wire instructions once given unless within protocol
  - No changes in communications process unless verified
  - No deviations from protocol

Risks and Insurance

- For Lawyers
  - According to the gospel of Mike Kennedy
  - Lawyers should not count on sympathy from disciplinary authorities if a lawyer falls for a scam
  - Scams are sufficiently well known that everyone should be on guard
  - You will have to replace the misdirected funds immediately
- Insurance Coverage
  - Business risk policies do not cover cyber-liabilities
  - Coverage by endorsement or separate policy
  - Read the policies carefully – what events are covered – employee misconduct, loss as a result of system breach,

Were Chapter 2 facts a breach?

- State statutes on notification
  - Vermont
  - State of client / customer residence
- Notification of client and Attorney General's office
- Where did the breach occur
  - Nyse & Knotty – notify all clients of breach
    - Only notify affected client
  - Client system – any responsibility to notify
- New profession – Breach Coach!

Chapter 3

!!Security Warning!!

We have detected that your security system has been penetrated. To preserve the sanctity of your digital information all of your datas are encrypted by our technical services department for your protection.

You must first establish your identity by providing your login credentials for you emal server and network and also pay our reasonable fees and costs for providing this service to you're company.

Our fee is .3 Bitcoin.

Our technical services department is standing by at

+8 80 4 8112110

To Assist you with the purchase of Bitcoin and the process for transferring Bitcoin to our account. This is a limited time arrangement and you must respond within 24 hours of receiving this message or we will assume you no longer need you're data and remove it to permanent storage on our servers.

Worst Possible Case --- RANSOMWARE – Best Case- Zombie

- Ransomware
- Contributing to the delinquency of a computer, refrigerator, router, camera, baby monitor, or other internet connected device
- Browser hijack
  - Browser locked on a specific site
  - System locked with ransom demand
- System hijack

Preparation – Backups
Best Antidote to Ransomware

- How many backup systems do you need?
  - At least two, probably three
  - Nearline – a USB drive connected to a computer or server with a shadow copy of your current files
  - Online – your backup in the cloud
  - Offline – at least one backup that is not regularly connected to your computer / network unless the backup is running

Second Best Antidote

- Malware protection
- Full time scanning – commercial grade protections
  - No endorsements but – McAfee, Norton / Symantec, Bitdefender, Webroot,
- Alternate periodic scan
  - Endorsement – MalwareBytes – paid version ($29.00) per year
  - At least once every two weeks, once a week is better
- Check Logs – frequency of hits
- Where are infections coming from?
  - Bad internet hygiene
  - No non-work related websurfing on work computers
  - Links in bad emails – train users to look for hints

Preparation - Training

GOOD PASSWORD HABITS

- Force Change Passwords – 90 – 180 days
  - Workstations, servers and services (administration accounts),
- Routers and perimeter hardware
- Strong Passwords
  - Minimum should be 17-20 characters
  - Formula to create password / passphrase
  - Color/Animal/Fruit – add numbers or symbols
  - No information I can find about you on Facebook
- NO REPEATS or REUSE

Response

- Do the folks in your office know what to do when something bad happens?
  - I think I clicked on a bad email; or
  - I think I clicked on a link in a bad email
  - My computer says that the FBI is going to arrest me for child pornography unless I send them $300 in iTunes gift cards.
  - You discover you wired money to a fraudulent account
- You should have a response plan for as many things as you are willing to put time into developing.

Final Questions

Thanks for Coming