ASSURED ENTERPRISES INC

Serious Cybersecurity™

NEXT GENERATION CYBERSECURITY

Cybersecurity . . . Tested, Trusted, Transformative

Cybersecurity, the Law, and Protecting America's Cities

October 2019

What is Cybersecurity?

- Goods and Services? Solutions? A Necessary Evil?

- What Does An Effective Cybersecurity Strategy Entail?
  - multiple layers of protection, usually spread across networks, computers, software, and data.
  - Risk Identification, Measurement, Management and Mitigation

- What Do Cities Need in Cybersecurity?
  - Defeat Phishing, Ransomware
  - Satisfy Compliance, Advance Training
  - Manage different technologies, platforms, systems, software across many departments

- In the end, everyone needs **to feel** the benefits from an effective cybersecurity approach.

Unique Threats that Cities Face

Many cities are vulnerable to a complex supply chain issue.

For example:

- 23 small Texas towns were hacked and then held for ransom
- All of the cities that were hacked used the same Managed Service Provider (MSP) for technical support
- Typically MSPs are used to monitor activity and fix issues, install applications and updates

As a result:

- When the cities were hacked, hackers deployed ransomware and encrypted data
- Since the backups were managed by the MSP, they were encrypted as well
- Estimated cost: $12 million and counting

Cyber-attack Against Baltimore

A cybercriminal group asked the city of Baltimore to pay $76,000 via ransomware.

The city wisely stated that paying ransom was not an option

Cybersecurity professionals reported that replicating the encryption key without the hackers help was impossible. Is that true?

As a result:

- Hackers held their computer systems for 36 days
- Billing systems went down
- Estimated cost: $18 million and counting

Cyber-attack Against Atlanta

Cybercriminal group asked the city of Atlanta to pay $51,000.

The city refused to pay the ransom.

As a result:

- Years of Atlanta Police footage from the patrol cars was lost
- This could compromise numerous DUI cases
- Other Data Losses
- Estimated cost: $17 million and counting

- Question: Were these Cities Non-Compliant with Regulatory Requirements?

Insufficient Service Professionals to Address the Threats

Too Many Threats

1 **365%**

Increase in detected ransomware attacks from 2018 to 2019

2 **13.275 Seconds**

Duration between ransomware attacks on businesses in 2019

3 **$11.5Billion**

Estimated damages from ransomware attacks by the end of 2019

4 **Only 10%**

of all cyber crimes actually reported each year

5 **Over 25%**

of all cyber insurance claims filed last year were because of ransomware

Too few professionals

1 **300,000+**

Unfilled cybersecurity jobs in the US alone

3 **3.5Million**

Unfilled cybersecurity jobs in the US by 2021

2 **80%**

Of companies don't believe their cybersecurity candidates have the skills needed to protect against a breach

4 **Estimated75%**

Of IT infrastructure will be controlled by 3rd parties such as MSPs and MSSPs by 2020

How Did We Get Here?

Why are we in the mess we're in?

- Compliance Does Not Equal Security
- There is a battle underway in cybersecurity goods and services
- Old School vs New School (Cutting Edge) Cybersecurity

What is the difference?

- Old School relies on: rule and signature based systems
- Fatalism
- Maintenance to Keep the Trains Running and New Products To “Prove” We Are Doing Something

Example:

- Firewalls and anti-virus protection are all rule and signature based
- All the hackers have to do is determine the rules and do something different
- Getting around a firewall is not difficult
- Circumventing anti-malware protection is also not difficult

Cybersecurity in the IT Department

Using the old school way of thinking, cybersecurity is a problem for the IT department.

In reality, this is how cybersecurity works when handled by IT:

- IT is there to keep everything running
- Their goal is to get you back online
- They are not concerned with what happened, nor how or why it happened
- They want to know, “What is the situation?” and “What kind of work-around can we apply to get you back online?”
- How Do We Keep the Budget in Line With What the Non-Technical People Say We Can Spend?

Old School Cybersecurity

They are happy to give you consulting at or even below cost, but what they want is an exclusive cost.

- When you get hacked, they come in with a SWAT team of 16 people to fix the problem
- In reality, you only need 3-4 people, but you are paying for 16
- These companies provide senior engineers who are tasked with trying to keep people looking busy

That's how they make their money.

Old School Cybersecurity (cont.)

- There are publicly traded companies that do this
- This is old school paint by the numbers
- Results are largely predetermined before they arrive
- Squeezing facts into a report just so we can say we got it

This old school methodology relies on fatalism:

- They take a fatalist mentality—the hackers will always win
- Everyone gets hacked and there is nothing we can do about it
- They act like it's an Act of God
- They make their margins once an organization is hacked

New School Cybersecurity

New School Cybersecurity

New school cybersecurity uses a **fact-based**, rational system.

- They can identify and manage **risk**, getting your systems to meet or exceed proactive cybersecurity. Every organization is obligated to have an independent cyber risk assessment
- There is no false sense of certainty.
- New school approach can provide cutting-edge risk assessment—satisfy all Compliance Needs, Measure the Risk and Provide an Actionable Program for Reducing Risk which Non-Technical Team Can Understand and Decide On

Every risk assessment is comprehensive.

- They are gathering all of the facts
- There are no preordained results, facts drive action
- They are gathering 6 to 10 times more facts than the old school methods

New School Cybersecurity (cont.)

They will build and use a tool that will objectively show relevance of those facts.

When you gather info, you have to do it differently, you have to talk to lots of people.

You have to look at:

- The documentation, systems, business processes, training program for the company
- The business plan for the company
- When a company is looking for an acquisition, you have to take a different approach
- When companies hold information that certain threat actors want, you have to adjust your strategy

A Triumvirate of Trusted Advisors

Every major organization or city needs to have a triumvirate of trusted advisors.

This triumvirate will include:

- Cybersecurity Knowledgeable Outside Legal Counsel
- Cybersecurity engineering firm
- Knowledgeable insurance broker or adviser

You need all of these on retainer.

A Real-world Example Or The Kind of Story You Can Take Home

A State Insurance Commissioner asked us to conduct a cyber risk assessment of a small insurance company.

The company's specialty was managing Health Savings Account and Flexible Spending Accounts.

And the Plot Thickens…

New School vs. The Bad Actors

With the new school methodology, you have to put your head into the mindset of all of the bad actors from nation state to amateur hackers.

New school companies need to think like cyber criminals:

- What do I want?
- What do I need?
- How do I go get it?

Typically, a bad actor might skip over a target if it’s not easy to compromise. (Unless they have a specific mandate to go after that target.)

Generally if criminal actors can't get in easily, they're gone.

What Derails Most Organizations?

What derails most organizations from understanding the risk assessment?

- A fundamental confusion between compliance and security
- Understand Your Data. Understand Your Threats. Understand Your Risk
- In order to be secure, you need to put yourself in the mind of the bad guys
- To do that, you need facts
- Measurement
- Common Language for Communication
- Trust to Embark on a Plan of Action

Common Law Standard

- Over the last several years, the notion of proactive cybersecurity has crept into the courts
- Common law covers how an organization is supposed to approach figuring out how much security they need
- Every organization that is regulated is required to undertake all **commercially reasonable proactive standards**
- They have to do a cost benefit analysis based on the risk. They have to find out if the cost is commercially reasonable or if it costs too much
- This is especially true when it involves HIPAA and HITECH

Enforcement for HIPAA and HITECH is Increasing

- A common problem occurs when entities (i.e. Business Associates) conclude that since their business type is absent from one of the HIPAA categories, they don't have to worry about HIPAA
- In reality, HIPAA covers a wide range of organizations, especially those that work with protected health information (PHI)
- Industry perception indicates that in the past, Health Information Technology for Economic and Clinical Health (HITECH) compliance has not been strictly enforced
- However, Washington is now paying closer attention and performing audits when entities are willfully neglecting the HITECH act

HIPAA and HITECH Affect More Than Medical Organizations

- Business Associates need to conduct a thorough and accurate HIPAA risk assessment in order to meet the requirements of the HIPAA security rule
- This includes every organization that receives, creates, maintains, or transmits PHI
- This not only applies to medical facilities but also consultants, business associates, and vendors

How Can You Trigger HIPAA/HITECH Enforcement?

- In 2013, the HITECH Act made business associates directly liable for certain types of HIPAA compliance

- Health & Human Services' Office for Civil Rights (OCR) has outlined **10 instances** where they will ensue enforcement:
  1. Not complying with the requirements of the HIPAA Security Rule
  2. Using and disclosing PHI without permission
  3. Under certain circumstances, not providing an accounting of disclosures
  4. Not providing the HHS secretary with proper records and compliance reporting
  5. Not entering into Business Associate agreements with any subcontractors that receive or create PHI

How Can You Trigger HIPAA/HITECH Enforcement? (cont.)

6. Not notifying Covered Entities or Business Associates of a breach
7. Taking action against an individual that is filing a HIPAA complaint
8. Not disclosing a copy of electronic PHI to covered individuals or entities
9. Not making reasonable efforts to allow the minimum level of access to PHI needed for disclosure, request, or use
10. Not taking reasonable steps to address a violation of a subcontractor's business associate agreement or material breach

Common Violations That Result in Fines

- Data breaches
- Lack of training
- Stolen or lost devices
- Not disposing of PHI properly
- Portable devices that don't have PHI encryption
- Third-party PHI disclosure
- Not performing regular risk analysis across the organization

Penalties for a HIPAA Violation Can Be Severe

- Tier 1: An entity is using reasonable due diligence and is still unaware that HIPAA rules have been violated = $100 – $50,000 per violation
- Tier 2: An entity should have known about the violation using reasonable due diligence = $1,000 – $50,000 per violation
- Tier 3: An entity shows willful neglect of HIPAA rules, however it is corrected within 30 days after being discovered = $10,000 – $50,000 per violation
- Tier 4: An entity shows willful neglect of HIPAA rules and made no effort to fix the violation within 30 days after being discovered = $50,000 per violation
- Each of these has a maximum of $1.5 million per year

The Real Cost of an Audit

- A conservative estimate for employees is roughly $100 per hour worked
- This includes the cost of employees that are collecting salaries and benefits

Direct cost of an audit

- HIPAA gap assessment: $24,000 – $34,000
- Full HIPAA audit: $30,000 – $60,000
- Validated HITRUST assessment: $100,000 – $160,000

Indirect cost of an audit

- The biggest factor in indirect cost is time
- Here's an estimated amount of time spent for all employees for each type of audit:
  - Gap assessment: 40 hours
  - Full HIPAA audit: 100 hours
  - Validated HITRUST assessment: 400 hours

Tips for Passing an Audit

- Here are some best practices to help you pass your next audit:
  - Fully document your security, training, data management, and notification plans
  - Create password policies
  - Encrypt files and databases that contain PHI (While this isn't a HIPAA requirement, it is a best practice and suggested.)
  - When accessing sensitive data on the web, use SSL
  - Minimize access to encrypted sensitive information
  - Use VPN for remote access
  - Create a documented disaster recovery plan

Tips for Conducting a HIPAA Assessment

- A HIPAA privacy risk assessment is just as important as a security risk assessment
- Appoint a privacy officer. This person will identify organizational workflows and get a better understanding of how the HIPAA privacy rule impacts the organization.
- The privacy officer will map the flow of internal and external PHI and use that to create a gap analysis
- They will develop and implement a HIPAA privacy compliance program
- This program should be reviewed as suggested by the HHS

Getting the Right Data

A HIPAA Assessment Will Likely Include:

- Threat actions which could include risk associated with weather, personnel, and power related outages
- Documented physical, technical, and administrative safeguards
- Documentation for any hardware and software that contains PHI
- Encryption protocols that include data storage, email, devices, and wireless connections, etc.
- Documentation for physical security of facilities and workstations
- Liability insurance
- Guidelines for destruction and disposition of data
- How downstream business associates will be monitored

Tools for Scanning

- Companies need to scan on a periodic basis with the following:
  - IDE scanner: This is a source code scanner and only helps when creating software.
  - Network scanners: They look for network connections and determine how the hardware and software interact with each other.
  - Deep software scan: This scan focuses on software resident in your system and helps to identify known vulnerabilities in software.

Equifax Hack

One example is the Equifax hack.

- Equifax adopted a new Apache Struts system for reading data.
- It contained a known vulnerability.
- Without a deep software scan, they had no technique to figure out what the problems were.
- However, it was publicly known that a hole existed in the software.

How Often Should You Scan?

- 70% or more of cyber-attacks exploit known exploits
- This is the most common technique and how WannaCry, Petya, NotPetya, etc. worked
- A deep software scanner will show vulnerabilities and tell you how to fix it
- Periodic Scanning Program
- New vulnerabilities are being found every week
- This is why you need to do this every few weeks or months, not once per year

The Good News

- Solutions are available
- They can be tailored to your budget and circumstances
- They can satisfy your Compliance and Legal standing
- They can help you make sure you're prepared for dealing with the insurance companies
- Insurance Gap Analysis
- Solutions ARE Available

ASSURED
ENTERPRISES INC
Serious Cybersecurity™

Contact:

Stephen M. Soble

Assured Enterprises

ssoble@assured.enterprises

www.assured.enterprises

+1.202.821.9058