
A
CYBER
SECURITY
ROAD
MAP
INNOVATE
E-COMMERCE INC.

INTRODUCTION

Most companies are aware they need to do something to protect themselves from cyber-attacks. But most resist doing anything, not because they don't want to move forward but because of budgets, resources or they don't know where to begin. The four areas of Cyber Security are **Protect, Detect, Respond, and Recover**. These tasks can be done independently of each other, however if you create a Cyber Security Plan, you will find that they are all interrelated. The following endeavors will improve your cyber security and can be completed utilizing minimum dollars and resources. The first place to look is where your company is the most vulnerable.

1. CONDUCT A RISK ASSESSMENT

If securing your company's data is one of your projects for this year, you need to plan for how your budget dollars will be used. Where do you start? What do you secure? Where is the best place to spend your IT budget dollars to get the most "bang for the buck?" Begin with a Risk Assessment. Why? Because the biggest problems most companies face when putting together a security plan is – they don't know what they don't know. Questions such as:

- *What data should be protected?*
- *Where is my environment most vulnerable*
- *I have a firewall, antivirus software and monitoring logs, what more do I need?*
- *What are the relevant threats?*
- *Can we detect a breach if one has occurred in our company?*

A risk assessment can be done using internal resources, but this may not give you the best results. A company that specializes in security can look at your organization from the outside in. They will evaluate the entire enterprise, not just the IT environment or from an IT perspective. They will help you answer the aforementioned questions plus, assist you in deciding where to spend your budget dollars to achieve the greatest value and security.

If your budget does not allow you to hire a third party to do your Risk Assessment, then you need to include the following tasks:

- *Conduct Executive Interviews*
- *Create a detailed Threat Analysis*
- *Learn and document all compliance requirements*
- *Prioritize Recommendations*

Conduct Executive Interviews

The first task in a risk assessment is to interview management from all departments. This will help you determine what information they identify as critical, sensitive, and necessary for them to conduct business. This will help you answer the first question, "What data should you protect?" Once you have established what information is important to every department you can begin the next step.

Detailed Threat Analysis

A *Detailed Threat Analysis* includes application and infrastructure threat analysis. Once you have determined what information is important to each department, you need to determine what applications and infrastructure supports this information. Determine what is in place currently to protect this information from a breach. Who has access to this information? For example, does the sales department have access to only the applications that support sales?

Do administrators in the IT department understand their responsibility for the information they can access? What about anyone with remote access? Are the policies and procedures in place that ensures that they can remotely access only the information they should? With the introduction of cloud-based applications, analysis of these applications must also be completed. If you think of cloud-based applications, every user is now a remote access user, where a different set of security rules, policies, and procedures will need to be put into place. Make sure these applications are included in your risk assessment. Many companies make the mistake of assuming that the cloud-based application company will set up the correct security. In most cases, setting up access and security is your responsibility, not the cloud-based application company.

Compliance Requirements

Do you have to adhere to any compliance requirements? This includes regulations such as HIPAA, GDPR, PCI-DSS as well as Federal, state, and local regulations. Many companies do not realize that if they are breached, there are Federal, state, and local laws and/or requirements a company must follow. If you don't know what they are for your company's location (s), this must be documented. During a risk assessment is the time to research and document these requirements, not during a data breach. Once all the requirements and compliances are known and documented, you must do a gap analysis of what you are currently doing and what you need to do to be compliant.

Recommendation

Once you have conducted the interviews, performed a detail threat analysis and document-ed all the compliances and regulations, you can prepare your recommendations. How you prioritize the recommendations will depend on you. Some companies will prioritize the recommendations based on greatest risk to the company while others start with the ones that can be completed quickly. However you prioritize your list of recommendations, your key to success is to minimize your risk of a breach by completing all of the recommendations. This is when an outside company can help. They will help you prioritized the recommendations list and assist you in implementing a solution and/or assist you in finding the right software or hardware needed.

2. CLASSIFY YOUR DATA

Before you start to purchase or upgrade software and hardware to protect your company from a cyber-attack, you need to determine what data is most important for you to protect. Or, a better approach, ask yourself what data do you need to conduct business? This answer may vary from department to department which is why this project must include the entire company from a business perspective, not from an IT perspective.

The first place to start when classifying your data is to form a team. This can be a few as 2-3 people but must represent several departments and not just personnel from your IT department. This team needs to interview each department to determine several important requirements.

- *What data is most important to them?*
- *What is the sensitivity of their data?*
- *What is the value of the data to that department and to that enterprise?*
- *How long can they perform their duties without access to their data?*
- *What data can they access?*
- *Does anyone in their department have and/ or need remote access? If so, how is remote access given and monitored?*
- *How is their data shared interdepartmentally, internally within the company and externally?*
- *Does their data need to be compliant with any regulations such as HIPAA, PCI, EU or others?*
- *How/where is their data stored?*
- *How often is their data backed up?*

Once all these questions are answered, for all your departments, you can now start the process of classifying your company's data. You will have a clear picture of the value of each department's data, what is important for them to do their job and how long they can continue to do their job without access to their data. You have blueprints of what data must be available as quickly as possible and what data can be delayed to come online if a breach occurs. In addition, you will learn how and where valuable and sensitive data is accessed and stored. You need to look at all data; live, in motion, and at rest. Live data is emails, files, and documents that are created and handled right now. Next, you need to look at data in motion. This is data sent and received internally and externally, populating all web applications, and shared throughout the enterprise. Data in motion includes data downstream. Where does the data go once it leaves a department or the enterprise? Data at rest is all data stored. This would include data in databases, within applications, backups, and cloud services. You will also have a clear picture of who does and who should have access to each type of data.

Another important element of classifying your data is to ensure you are compliant with all regulations. If you have to be HIPAA compliant, are you protecting, sharing, and storing data to meet the requirements? If not, now is the time to document what changes need to be made to become compliant and set a timeframe for this to be completed.

This is the beginning of your Security Policy and will become part of your Incidence Respond Plan. You must develop a plan to make sure your policies and procedures reflect the needs of your enterprise to protect your data and get back online.

If you have the budget to hire a third party to help with the classification of your data, this is also an option to consider. The advantage of a third party performing this project -- you will get a better picture. A third party will look at it from outside of the enterprise inward. They will look at the enterprise as a whole, each department individually, and how departments work and share data. They will not have any preconceived opinions of what data is sensitive, valuable or critical to the enterprise.

3. REVIEW AND UPDATE YOUR BACKUP PROCESSES

When was the last time you reviewed your backup policies and procedures? Better yet, when was the last time they were tested? The time to test your backup procedures is not during or after a cyber-attack! You need to know how you are going to recover from a data breach. Knowing, testing, and continuing to update you backup policies and procedures is an inexpensive way to ensure your recovery time is faster and less painful. Most companies fail to review their backup policies and realize during the recovery process, their backups no longer support the business.

If you have completed the classification of your data project, you can align you backup schedule to ensure the most critical data is available online as quickly as possible. Start your review by asking yourself questions about your current processes.

- *When are backups scheduled?*
- *Are backups both full and partial? If so, what data qualifies for full or partial backups?*
- *Who is responsible for the backups?*
- *Is your backup plan in compliance with all regulations?*
- *What is the timeframe for the backups? Does the backup schedule align with the timeframe the users can go without their data?*
- *What happens to any data lost between backups?*
- *Is critical data backed up and stored differently than less critical data? If so, how?*
- *Is the backup done to a local drive, remotely over a LAN or wide area network?*
- *Who is responsible for verifying the backups were completed successfully?*
- *Who is notified if the backup fails and what is the procedure when it fails?*

After answering all of these questions, you need to update your backup policies and procedures. This is a time consuming project, it can be completed with internal resources and with minimum expenditures. Complete verification of the entire backup and restore processes are critical. Develop strategies with the appropriate resources and personnel, and then test them. During the test, document everything that went right and wrong. Make all the adjustments to correct any errors that occurred during the testing. But don't stop there! Test again. Your backup policies and procedures are not finished until a test is completed with no errors. But you are still not finished. Part of your backup policies and procedures is to have regularly scheduled recovery tests. You should do this at least once a year, but remember, the more often it is done, the more confident you will be that you can recover from a data breach.

4. REVIEW AND UPDATE HOW YOU MONITOR THE LOGS FROM YOUR FIREWALL, DETECTION, OTHER SECURITY AND APPLICTION SOFTWARE

The first step in your monitoring process is to determine what applications running in your environment produces logs. Next, determine which logs are important to monitor. You may have invested in firewalls, Intrusion Detection

Systems, and other software and hardware applications that protect the perimeter of your environment. However, if you are not monitoring the logs generated from these applications, you are not receiving the full value of your investment. If you have determined you need to monitor an application that does not produce a log, you have to make a decision. Does the application need to be upgraded because you are running an older version and the upgraded version can now produce logs? If the current version does not produce logs, you need to determine what information you need to know about the application. Can you create a process to extract the information needed?

Don't make the mistake that many companies do when creating monitoring processes and procedures; they monitor everything. What generally happens in this case is that the intention is great but the follow through fails. The logs become too erroneous to monitor so they are no longer monitor any logs. A problem is missed because too many logs will not give an accurate picture of what is happening in your environment.

If you have classified your data, then you know which data is most important to protect. Thus, the first place to look is at what applications run, backup, store and has access to that data. If you have not classified your data, then start at your first line of defense, your firewall, End Point Protection and anti-virus software, and access control. If you have either Intrusion Detention or Intrusion Prevention systems, these logs are critical to monitor.

Log management and monitoring will help you detect a security breach within your environment. Research has shown that it takes an average of 208 days for a company to detect that they were breached. In addition, it takes them an average of 69 days to remove and recover from the breach. Protecting your environment and detecting a breach must be included in your security plan.

Protect Your Environment

Your first line of defense is the software and hardware that protects your environment. Make sure all of these are running the most current version. If they are not, upgrade to the newest version. Many of them have new features that protect your environment and produce better logs. If you are running the newest version, make sure you are taking advantage of the new features. Many times, a company will upgrade their hardware and/or software but will not utilize the new features. Many of these features provide better protection and logs that will help you secure your environment. Microsoft will send updates out and they can be automatically downloaded. If you are running Microsoft on any of your computers, make sure they are set up to do upgrades automatically. The same should be done to your anti-virus software. If you are not updating it, it cannot protect you against the new viruses, malware or other kinds of attacks. Remember the cyber attackers are continuously changing and improving the way they hack into your environment. Keeping your software up to date is one way to help to prevent a breach.

Intrusion Detention System (IDS) and Intrusion Prevention System (IPS)

Intrusion Detention System (IDS) monitors traffic at the network or hosts (device) level. The network based software (NIDS) is placed at strategic points within your network to monitor traffic to and from all the devices within your environment. All inbound and outbound traffic should be monitored. However, most companies do not monitor all traffic because it can slow down the network and impair the overall speed of the network. If you choose to not monitor all traffic, you must understand the risks you are exposing to your environment. Host-based Intrusion Systems are deployed in the host servers and analyze data that are local to the machine to identify unusual behavior (HIDS). It compares traffic patterns against a baseline.

IPS technology takes an additional step on monitoring that IDS does not. IPS will try to detect a problem. For example, IDS may detect an invalid IP address that is trying to access your environment, IPS will block it from gaining access to your environment. Another way to

think of IPS is the way that your email blocks invalid emails by placing them in either a spam or junk folder. IPS often sits behind the firewall to provide a layer of analysis such as:

- *Sending an alarm to an administrator*
- *Dropping malicious packages*
- *Blocking traffic from the source*

IPS was originally built as a stand-alone solution but now it is included in next generation firewalls. The main difference to remember between IDS and IPS is that IDS monitors the network to detect inappropriate, incorrect activities, while IPS detects intrusion or an attack and takes active steps to prevent them.

Log Management and Monitoring

Depending on the sophistication of the logs generated from each system, monitoring the logs could be relatively easy or difficult to spot an attempt or successful attack. You need to have a dedicated person monitoring these logs. This person must be trained to know what to look for to detect a breach or an attempted breach. If the person is untrained or not dedicated to monitoring the logs, a breach may occur and it will take you days, weeks or sometimes years to detect a breach. In March of 2018, American Express informed their card holders that used American Express for online travel purchases that Orbitz had been breached. (Orbitz is the engine behind American Express online travel.) The breach occurred in January of 2017 and continued until 2018. This meant Orbitz had been breached for over 700 days before it was detected. Why does it take so long to detect a breach? There are many reasons but most involve the company's lack of systems in place to detect a breach. Determining what logs are being generated within your environment and which ones need to be monitored is a great step to help detect that an attack was attempted or has occurred. However, detecting the breach is only the first step. The person monitoring the logs must know what to do next. Who do they notify? You need to have the processes in place to isolate the breach, eradicate it from your environment, and recovery to get back to business as usual.

5. INSTITUTE AN INCIDENT RESPONSE PLAN

Describing an Incident Response Plan could take an entire white paper. This section will give you an overview of what needs to be your response plan and get you started down the right path. Creating and testing an Incident Response Plan should be done now, before you have been breached. During a breach is not the time to develop one. The six major components of a plan should include; **Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.**

Preparation

How prepared is your company to protect your data and detect if a breach has occurred? Firewalls, IDS, IPS, and log management are some of the ways to guard against cyber-attacks. Classifying your data and ensuring your backup policies align with the time needed to get your critical data back online are other key components to protecting your environment. If you haven't done any of these yet, you need to start now. Not tomorrow or next quarter, but NOW! A lot of the preparation can be done in-house with your current staff. But you need to make sure they understand what their responsibilities are and what the overall objective of the plan is. They need to understand that it is okay to point out deficiencies and weaknesses in the current processes. If the team responsible for developing a response plan is afraid to identify problems in the current environment, nothing will change or be improved. A plan has little value if it is not put into action, tested, and continuously improved. This is not the time to have egos, departmental differences, or not wanting to change the status quo. This plan may be the difference between keeping your company's creditability, minimizing the risk, losing some of your customers or staying in business.

In your plan, you need to know who is in charge during the recovery process and who can and will make the final decision if and when needed. It is essential that the person in charge has been trained and has the support of senior

management. During the recovery process this person must be able to make decisions quickly.

Identification

Hackers have become very skilled and know that they rarely get caught. Plus, they have become so efficient in developing their code. They know many of the vulnerabilities in current software, which makes it easier for them to attack and harder for you to identify, recognize what type of breach it is, and where in your environment the breach has occurred.

Identifying the type of breach will help you determine how you are going to eradicate it from your environment. Probably the easiest breach to identify is Ransomware. If this has happened to someone in your company, they would have a message on their computer demanding a fee before they would return your stolen data. However, many companies have found that even if they pay the ransom, the hackers still do not return the stolen data. An important part of the identification process should include identifying the following:

- *The nature of the attack*
- *The extent of the attack*
- *What assets are infected?*
- *What data has been infected?*
- *Who has been infected – internal only and/ or customers, suppliers and other third-party partners?*
- *What are the implications of the attack on your business?*

What can be the cause of a large data breach? In 2017 The U.S. Department of Health and Human Services for Civil Rights (OCR) looked at the most common causes of data breaches that caused HIPAA compliance failures. This chart illustrates their findings.

Containment

Once you have discovered you have been breached, you must contain the effected section of your environment. It may be only one computer or it could have spread throughout your entire environment. Once the breach is contained, you must begin the process to identify if any information was lost , stolen and/or compromised. While you are determining the processes needed to remove the infection and restore your environment, you need to communicate to all the stakeholders and all entities that have been comprised.

You need to have people with the necessary skills to contain the breach to be able to take the following steps.

- *As soon as you identify the access point, disable all lines of connection to prevent further access or spreading*
- *Identify any programs, files or executables that have been installed from the breach*

Eradication and Recovery

Once the breach has been contained, you must make sure it has been completely removed from your environment. Focus on removing and restoring the affected systems. Determine what has been affected and how many steps need to be taken to ensure the malicious content has been removed. If only one department's data is infected, can you restore from the last backup? Or if the malicious content has spread company-wide, do you have to restore from the bare metal up?

Start your recovery with the following steps:

- *Run security patches and software updates for your operating system and applications. Many upgrades include security enhancements.*
- *Uninstall and reinstall affected files and programs. All files and programs that have been affected by the attack should be removed and reinstalled from clean backups.*
- *Initiate new login procedures for all affected parties. If you don't have strong password procedures, develop them. Include upper and lower-case letters, numbers, and symbols. Institute a policy that requires users to change their passwords on a regular basis as well as using two-step authentication especially for sensitive and confidential information.*

Make sure in your Response Plan the processes and procedures needed to recover are documented to eradicate a breach from all levels of your environment. How quickly and

successfully your recovery will depend on how well you prepared before a breach occurs.

Lesson Learned

Testing your plan before a breach will expose weakness in your plan. This is the most important part of an Incident Response Plan and the part least performed. This will allow you to document what went right and what went wrong. Next, improve your plan with the changes that need to be made. Make sure the changes are documented. Don't forget to test again. I know you are reading this and probably thinking to yourself this will take a lot of time and resources. And it may. But what is the cost to your company if you do have a data breach and recovery time is lengthy? Test, retest and test again is your best line of defense against cyberattacks.

6. CREATE A BUSINESS RECOVERY PLAN

When companies think about a recovery plan they think of it only from an IT perspective. This is a big mistake and could cost your company a lot of time, money, customers, and even worst, going out of business entirely. While your IT department is working to restore your information and getting the company back online, you must continue to do business. This is where your business recovery plan is important and needs to be documented. The four major components of your business recovery plan are:

- *Develop a recovery plan*
- *Communications*
- *Lessons learned and improvements*
- *Retest*

Develop a Recovery Plan

The first task in developing a business recovery plan is to determine what processes and operations must continue while you are coming back online. If the average timeframe to recover from a data breach is 69 days, do you have a plan to continue to do business without some or all of your data over those 2 months? What is your staff doing during the recovery time? Do you have to lay people off, hire more, and/or have people work from home? Have you designated who is in charge of making decisions for the business during the outage? Have they been trained? Who is their backup?

If you have determined what processes have to continue during the recovery, how is that happening? For example, if you currently receive most of your orders electronically and cannot do so because of the cyber breach, can you manually take the orders by phone, fax, email or mail? Do you have to hire additional staff or have you trained staff to do this job if a breach occurs? You may remember when several hospitals around the globe were breached. They stopped all surgery except for emergency surgery. What are your emergency processes that must continue while you are recovering from a cyber breach? Once the emergency processes are determined, the process for them to continue with or without access to their data must be documented.

Communications

As soon as you realize you have been breached—time is critical. You must notify all relevant stakeholders, authorities, partners, customers, and any and all entities compromised as quickly as possible. A crisis team is critical! If there is no communications team, the likelihood of confusion, errors and the wrong message is a major risk. Designating the CEO as the spokesperson is a great idea because it indicates to the public the issue is taken seriously. However, make sure the message is well scripted because the CEO may not have the technical expertise. Therefore, the CEO may not be able to explain the technical aspects of the recovery. Make sure the information in the first message is correct and accurate. The most important communication error is timing. Errors are made if communication is too early or too late. It is imperative that you know the required timeframe to comply with the law in your state and local regulations. Know what your Federal requirements are when reporting a data breach. During recovery is not the time to research what your Federal, state, and local requirements are, they should already be documented in your business recovery plan.

How are your customers going to reach you during your recovery? Do you have toll free numbers set up that can handle the volumes of calls you will received if there is a breach? If you have customers that are trying to receive information and cannot get through to anyone at your company, it will only make the situation worst. Don't forget your website. Do you have a message on your site explaining what happened and how you are responding and recovering from the breach? You need to make sure every means for communications to the public has the same message and information.

Monitoring news and social media as well as your call center is just as important. Social media reveals what customers are thinking and saying about your company. News media will tell you if the information was clear and understood or if more information is required to make sure the correct message is being received.

Lessons Learned and Improvements

Preventing a cyber security breach is not only the responsibility of IT, and everyone in your company should be part of the solution. Build a crisis team which includes team leaders from each department. They need to be responsible for communication internally and externally. They are also responsible for documenting what went right and what needs to be improved in the recovery plan. Hindsight is 20/20, so use this to your advantage. Was the person that delivered the message, the right one for the job, were you too quick to get the message out, how well did you support your customers during the recovery? Was the first communication to the public accurate and ahead of any leaks? Were you able to conduct business during the recovery in the way you thought you could?

Answering these questions and making improvements will make your recovery plan better and your recovery time shorter. And of course, don't forget to retest again and again. We live in a world where countries are paying people to purposefully attack US companies. There don't care how big or small you are, they only care that they can breach your environment. The more prepared you are, the less damage and faster recovery you will have.

7. SECURE HOW YOU SHARE FILES

Ransomware, malware, Denial of Service (DoS) attacks, or viruses, are constantly attacking your critical and confidential information. Insider threats continue to plague business. In the past, insider threats had been focused on disgruntled or terminated employees. However, based on studies done over the past two years, incidents have been due mainly to careless staff. Employees have opened attachments with embedded malware and spread it throughout the enterprise or responded and shared critical and/or confidential information to a legitimate-looking email. Depending on which research paper or news article you read, most will quote that 85% to 95% of all security breaches occur because an employee was phished. This means that somewhere in your company an employee clicked on an email attachment, an ad on social media or a phishing email that allowed anything from a nuisance virus to a ransomware virus into your company's environment.

The main reason why insider threats are a top concern among cybersecurity experts is because it is a people issue not a technological one. It is easy to bypass security when you have negligent employees. Your employees share your company's information continuously all day, every day. Are you confident that they are not sharing critical and/or sensitive information publicly through email attachments, unsecured file sharing solutions, or other unsecure ways? You need to have an enforced policy that outlines how your employees share information internally and externally. Train your employees regularly on cyber security. Help they become "cyber security smart" to protect their personnel information and your company's information.

Not only do your employees share information all day, so do your applications. Your business applications are large investments and most companies do not implement them to enable them to reach their full potential. To accomplish this, they need to be integrated with other

applications, and more importantly, they need to be integrated with the applications of your customers, partners, suppliers, third party providers, and government agencies. Each application needs to "interface" to and from each other accurately, timely, and securely.

The reality is that most enterprises experience a countless number of problems setting up and managing their application interfaces. Properly setting up and managing interfaces can be arduous and time consuming. When setting up interfaces that send information outside of your company, ports are open in your firewall. Securing these opening are often times skipped in order to get the communications completed to meet a deadline. No one goes back to complete the task of securing the opened port thus leaving your company vulnerable to a breach. You will need staff to be trained with the expertise in networking protocols, security methodologies, and best practices for tracking and troubleshooting all the connections you need to support all your application interfaces. You also need to make sure someone is monitoring all your interfaces to ensure there is no attempt to or successfully breach your environment.

Another way to evaluate how you are sharing your information is to look out how can you prevent data loss? Data loss can happen by:

- *Email*
- *Unsecured file sharing*
- *File (or interface) transfers*
- *Backups*
- *Paper*

Email – Do you know what information your employees are sharing through attachments or within the body of the email? Are they sharing critical or sensitive information or violating compliance regulations?

Unsecured file sharing – Are your employees using an unsecure file sharing solution? Many in the marketplace today are not secure. In their terms and conditions, they state that they can share any information placed on their servers with other third parties. Your employees may have given an outside company the right you share you sensitive, critical, or private information to an unknown third party.

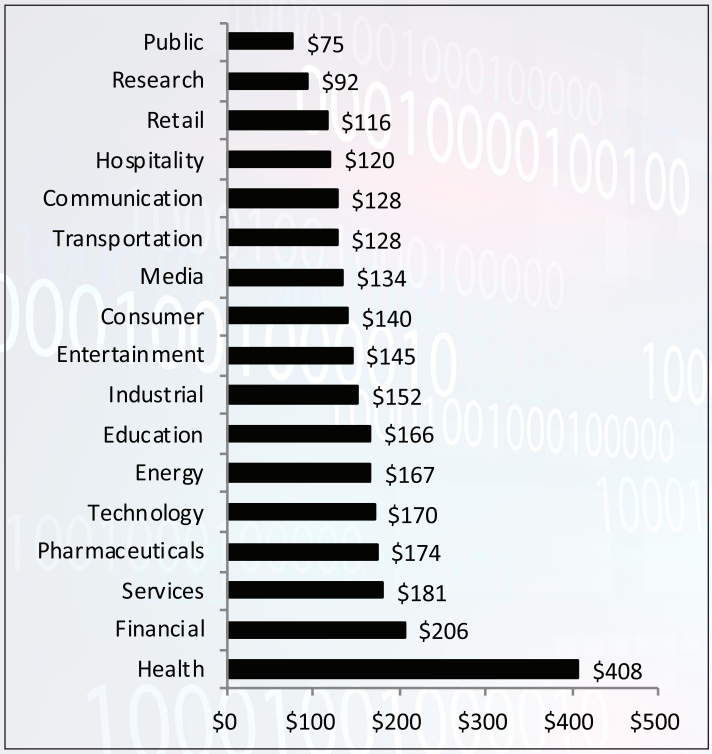
File (or interface) transfers – Who controls how file/interface set ups are done in your environment? If a new port is opened in your firewall, did they follow the procedure to ensure that port is secure? What type of protocol was used? FTP is often used to set up a file transfer because it is easy to do, yet it is the least secure and easiest to breach.

Backups – When was the last time you tested your backups? Does your backup schedule match your business needs? If you have completed a project to classify your data, has your backup schedule been reviewed and modified to reflect the needs of data classification? Also, where are your backups stored, who has access to them and who is notified if a backup fails?

Paper – In this electronic world, paper is often forgotten. One of the most vulnerable aspects of printing is the physical documents. Important, sensitive data is often printed and left somewhere unattended. Make sure all documents are shredded. But the paper document is not the only vulnerability. Now printer security is about data in transit. Protecting data in transit anywhere in your environment needs to be secured even data going to the printer as well as the actual printed document.

Summary

Cyber-attacks are happening all day, every day. Foreign governments are paying people to indiscriminately try to hack into US companies and government agencies. As a result, cybersecurity spending is on a pace to eclipse the $1 trillion mark by 2021. In addition, the cost of a data breach per document continues to rise. In their 2018 Cost of a Data Breach Report, IBM and the Ponemon Institute found that healthcare data breach costs average $408 per record, the highest of any industry for the eighth straight year. The following chart illiterates the cost of a document by industry. While the cost of a document in the Consumer industry it $140 per document, if 50,000 of your documents were breached, the total cost would be $700,000.



If you have not started a cyber security project, now is the time to start. You don't need a large budget and can do a lot of the work with internally resources. The FBI has stated, "It is not if you will be breach, but when". The more prepared you are now the better chance you have at surviving a breach.

Karen Puchalsky, Founder, President and CEO of Innovate E-Commerce has led the Pittsburgh-based company through over twenty-one years of accomplishment and prestigious recognitions. In 1997, Innovate E-Commerce is a global provider in supply chain managed services, secure communications gateway and secure file sharing enterprise solutions for small to medium businesses (SMB) and Fortune 1000 companies. Karen conducts monthly webinars on Cyber Security and has appeared on local radio and TV talking about Cyber Security.