Cyber Insurance

Businesses often ask Go West IT (Information Technology) if they should obtain cyber insurance and, if so, what kind of coverage, how much coverage, and how they should go about obtaining coverage. This article seeks to help educate small businesses about what cyber insurance coverage accomplishes for a business, and how to go about obtaining cyber insurance.

Cybercrime risk has increased dramatically for two primary reasons. First, nearly all businesses are now heavily reliant on technology to conduct day to day business operations. Second, cybercriminals have monetized criminal acts to the point that it is a multibillion-dollar industry with a relatively low risk of being caught or prosecuted. In addition to cybercrime being very profitable, it has also become increasingly simple because industrious cyber criminals now offer cybercrime as a service to less skilled criminals. This development further distances the skilled criminals from the crime and removes the barrier to entry for less skilled criminals.

Not long ago, cyber insurance coverage was not much more than a rider of a general liability policy or perhaps some protection for directors and officers on a D&O policy. Now, cyber insurance not only provides significant risk transfer but also provides important services to a business when they experience a cyber incident. These services are provided to reduce liability for the insurance carrier and have the benefit of reducing the impact of a cyber incident on the business. Services covered by and sourced through insurance carriers often include the following:

- Incident response services in the form of legal, forensic, and technical expertise to guide businesses through a cyber incident.
- Data recovery and/or data reconstruction services.
- Ransomware negotiation and payment services.
- Root cause analysis for the purpose of determining how to avoid subsequent incidents and for the purpose of helping to determine contractual liability for a data breach or data disclosure incident.
- Malware removal and remediation.
- Data breach notification services.
- Credit monitoring services for individuals whose Personally Identifiable Information (PII) may have been exposed in a breach.
- Specialized legal guidance regarding regulatory and/or data privacy reporting requirements.
- Public relations services to minimize business reputation damage.

Risk Management Strategies

Insurance companies began offering cyber insurance in the 1990s in response to risks that arose from business reliance on technology. Early coverage focused on risk transfer related to media (data storage), data processing, contractual liability, and business continuity risks. Cyber insurance still provides risk transfer opportunities related to these traditional IT risks, but most small businesses now think of cyber insurance in the context of risk transfer AND risk mitigation as it relates to cybercrime risk.

Risks associated with technology are vast and only add to the broad range of risk that business owners deal with every day. There are many ways to deal with business risk and cyber risk. Following are the most common strategies:

- **Risk Avoidance –** The decision not to use or engage in a particular activity for the purpose of simply avoiding the risk.
  - Avoiding technology entirely might not be an option but avoiding risk should be considered as businesses adopt new technologies. For example, a business might avoid the risk associated with an on-premises server failure by using cloud services. To be sure, utilizing cloud services will introduce different risks but it might be more easily mitigated. So, think about risk avoidance as you consider your IT infrastructure and IT strategy initiatives. You might be able to avoid some risks all together.

- **Risk Mitigation –** This is the act of conducting risk analysis to identify risks and then reducing risk by implementing additional policies, procedures, and controls. Risk mitigation will rarely eliminate risk but may reduce risk to an acceptable level.
  - Technology risk mitigation can be accomplished through regular reviews of vulnerabilities and criminal attack vectors and then working to constantly improve by closing gaps identified in the analysis process. This often requires assistance from a good IT managed service provide or managed security service provider.

- **Risk Acceptance –** This is the act of recognizing a risk that exists and simply choosing to accept the risk. Risk mitigation and risk acceptance are often combined when mitigation does not eliminate a risk. A business may choose to accept risk that remains after mitigation.
  - Nearly all businesses accept some IT risks. Unfortunately, not all businesses are aware of the risks they've chosen to accept. Risk acceptance is fine provided that key stakeholders know and understand the risks they have decided to accept.

- **Risk Transfer –** This is the act of transferring risk to a third party and in most cases, this is the role of insurance. Risk transfer is a viable strategy, but it is rare that risk transfer is the only solution used by a business.

When it comes to transferring IT risk, qualifying for a good cyber insurance policy most often require that a business has at least mitigated the most prevalent risks.

Cybercrime Risk - The Threat Landscape & Risk Mitigation

Cybercrime is prevalent because it is easy, profitable, and the likelihood of being caught or prosecuted is very low. Cybercrime is now also a mature industry made up of organizations managing 24/7 crime operations with as much a focus on efficiency and the bottom line as any legitimate business.

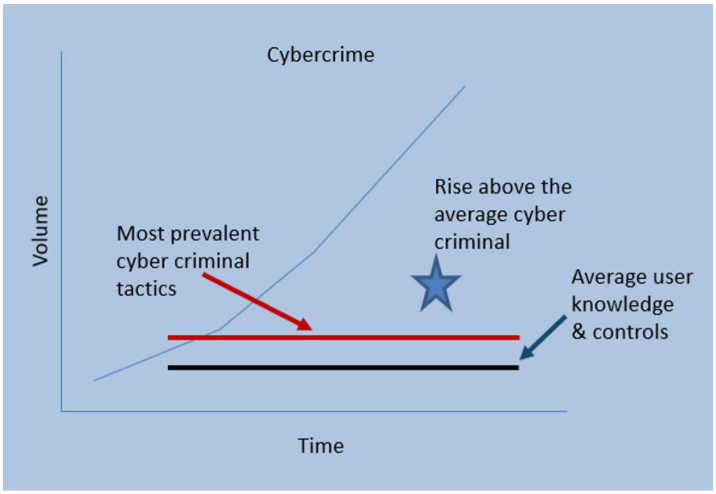
Cybercrime efficiency has resulted in increased risks for even the smallest businesses. Data ransom payments of $1,000 - $200,000 per event are very lucrative if accomplished efficiently by front line crime workers who use software as a service (SaaS) to deliver malware payloads, demand ransoms, collect payment, and send decryption keys. Personal data stolen from legitimate businesses is bought and sold on black markets for pennies a record. Cybercrime organizations buy this data and launch automated horizontal attacks against broad swaths of unsuspecting consumers. Gone are the days when a large payoff, and thereby a large target, was required to justify the amount of time, effort, and expertise required to perpetrate a cybercrime. Cybercrime has been democratized and no business, large or small, should consider themselves anything but a cybercrime target.

Cyber criminals are rarely pursued or caught due in part to the sheer volume of crimes relative to criminal justice resources. If caught, prosecution can be complex and expensive because crimes are often committed across state or international borders. Prosecution of high value international cybercrime organizations is extremely difficult and requires significant resources and multi-jurisdiction cooperation. Criminals are often prosecuted under centuries old chattel laws with pitiful consequences in relationship to the crimes committed. To make matters worse, some of the most prevalent and successful threat actors are sponsored and protected by nation states.

The combination of relative ease, high profits, and low risk has resulted in a dramatic rise in cybercrime with no end in sight. The good news is that businesses can dramatically reduce the likelihood of falling victim to an attack by employing controls to mitigate the easiest and most common attack vectors.

Graph A, devised by Cynthia James, CISSP, CCSP, depicts the threat landscape in terms of average user knowledge and business controls relevant to where most cybercriminals operate. Cybercriminals, in the interest of efficiency and the greatest return on investment, operate just above the knowledge level of average users and typical business controls. A business can dramatically reduce the likelihood of falling victim to a cyberattack by implementing enough controls and user education to rise above the crowd.

Graph A:



As of the writing of this article, the most prevalent and easily mitigated cybercrime risks are:

- Social Engineering Threats
  - Phishing – The act of a criminal enticing a victim to compromise an environment by divulging sensitive information such as a username and password or executing malware via link or email born attachment for the purpose of committing a crime.
  - Vishing – The act of a criminal enticing a victim to divulge information via a phone call that might be used to perpetrate a crime.
  - In person attempts to gain sensitive information, access to sensitive assets or access to controlled areas.
- Ransomware attacks where a criminal encrypts data and holds the decryption keys for payment of a ransom that is almost always paid in crypto currency.
- Business Email Compromise (BEC) whereby a criminal gains access to a victim's email account.
- Compromise of known system and platform vulnerabilities.

The criminal intent of the above acts is most often driven by potential financial whereby the criminal entices or coerces the victim to send money, gift cards, or other things of value. In some cases, the intent is simply to gain data that can be monetized through identity theft, selling data to other criminals, and even corporate espionage. Business Email Compromise, for example, is thought by the US Secret Service to be at the root of billions of dollars in fake income tax refund fraud.

Following are some practical strategies for mitigating the risks associated with the most prevalent types of attacks:

- Social Engineering
  - Phishing
    - Implement systems to detect and draw attention to suspicious emails.
    - Conduct test phishing campaigns for the purpose of identifying phish prone employees.
    - Educate employees about the danger and train employees to recognize phishing attacks and tell them what to do if they suspect they have fallen victim to a phishing attack.
  - Vishing
    - Conduct test vishing campaigns for the purpose of identifying employees who are prone to fall victim to a vishing attack.
    - Educate employees about the dangers and train employees to recognize attacks and tell them what to do if they suspect they have fallen victim to a vishing attack.
  - In person social engineering attacks
    - Educate users about the risks associated with divulging sensitive data to anyone or allowing anyone access to secured areas including offices with live network ports or unattended computers.

- Ransomware
  - Backups, backups, backups. The best way to recover from a ransomware attack is to restore data from backup so that you do not have to pay a ransom to have data decrypted. Design, implement, and test a good backup and disaster recovery strategy.

- Business Email Compromise (BEC)
  - Implement Multi-Factor Authentication (MFA) for 100% of email accounts and regularly review users and access controls.
  - Harden email platforms by eliminating unnecessary or obsolete protocols and turning off features that might allow data exfiltration such as automatic email forwarding rules.

- Compromise of known system vulnerabilities
  - Routinely patch operating systems, third party applications, and system firmware (i.e., firewalls, Network Attached Storage (NAS) devices, wireless access points, server hardware…)

A good security focused managed service provider can aid in implementing and maintaining all these risk mitigation strategies and more.

Once a business has done what it can to reduce risk, cyber insurance can play a key role in reducing the remaining risk to an acceptable level through risk transfer.

The Evolving Role of Cyber Insurance

Cyber insurance policies require that the carrier be notified of potential claims. In the past, this notification may have come well after the fact and perhaps even after an event had been dealt with. Now, insurance policies often provide services designed to help businesses deal with a cyber incident in stride and for the purpose of reducing the operational and financial cost associated with an incident. So, notifying an insurance carrier is often one of the first steps a business should take when they realize they are dealing with a potential cyber insurance claim.

A good carrier will be able to respond quickly with professionals who are accustomed to dealing with cyber incidents and who will guide a business through the process. The insurance claims person can help to bring in attorneys to address contractual issues and potential data privacy issues. They might also bring in a technical team to gather forensic information for the purpose of determining the attack vector, root cause, and how best to remediate the damage. Ransomware negotiation and payment specialists might be brought in to handle negotiations with a cybercriminal and even to handle the payment of a ransom in crypto currency if necessary.

It is important for businesses to understand that the insurance carrier will still conduct an analysis to determine if coverage is appropriate and anything shared with the carrier may be used later if a question of coverage arises. For this reason, the business may want to have their own attorney participate in discussions with the insurance company.

How Much Cyber Insurance is Enough?

One of the most common questions regarding cyber insurance is how much coverage a business should have. The answer is, as with many things related to information technology, it depends. It depends on the amount of risk, the size of the company, the capabilities of the company to deal with a cyber-attack on their own, the financial health of the company, and the company's risk appetite. To get to the bottom of this answer, a business should have an honest and thorough discussion with IT professionals and perhaps an attorney and an insurance professional to talk through the situation and produce a plan.

Following is a list of questions a business should consider when sizing up relative cybercrime risk:

- How much cash is managed by the business in a day, week, or month? How much cash loss can the business sustain?

- How many people and systems are involved in moving money in and out of the business? Another way to ask this question is, what is the attack surface relative to cash management and are adequate controls in place to manage the risk associated with cash management?
  - How many people and systems are involved in writing and signing checks, approving wires, transferring money between accounts, setting up vendors, approving payroll, and processing credit card payments?

- What would be the operational impact if the business lost data or applications? Think of word documents, spreadsheets, databases, technical drawings, accounting software, HR platforms, customer data, etc.
  - Where does the data live? On servers, in the cloud, in SaaS applications, on workstations, on Storage Area Networks…
  - Is the data backed up, what are the recover points (points in time), what is the backup retention (how far back), and what is the recovery time objective (how fast can the data be restored)?

- What would be the impact to the businesses reputation if a breach were publicized and thereby known to customers, employees, competitors, vendors…?

- What might be the regulatory risk in terms of penalties, investigations, cease and desist orders, increased oversight, or potential loss of ability to conduct business?

- Has the business conducted a thorough risk analysis and implemented controls to mitigate known cyber risk and how comfortable are owners or the board of directors with the remaining risk? If no, why not and are the owners or board of directors comfortable with the unknown risk?

- Has the company experienced a cyber incident in the past and if so, what did it reveal about the risks and ability of the company to manage that risk?

The above questions might seem to be an argument for purchasing as much cyber insurance as possible. On the contrary, it is the exercise of having discussions and considering answers to the questions that are important. Some businesses and individuals will have little cyber risk and a high appetite for risk. For other businesses, the discussion and answers to the questions might reveal significant cyber risk and very low appetite for risk.

It is not possible to mitigate 100% of cyber risk. Attacks are inevitable and successful attacks, which result in an incident, are a reality in today's technology landscape. Once a business has a feel for their risks and appetite for risk, a discussion with your insurance broker can help reveal how you might transfer the risk you are not able to mitigate or willing to carry.

Acquiring Cyber Insurance

Applying for cyber insurance will involve an application process through which the insurance company will seek to evaluate your relative risk based on revenue, number of people, types of systems, and your cybersecurity maturity compared to a broad set of industry data. It is extremely important to complete the cyber insurance application as thoroughly and accurately as possible. This may require that you get help from your managed service provider or IT department. Depending on the carrier, small details such as implementation of multi-factor authentication for email platforms, might result in premium savings.

When the insurance application is complete and when the premiums are being considered, it is important to evaluate the coverage relative to the premium. Following are example of questions a business might use to evaluate differences between policies:

- Does the policy include incident response management and if so, may a list of approved incident response vendors be reviewed?
- Does the policy include coverage for downtime resulting from a cyber incident? Most policies do not, and this may not be necessary, but it is an important question to ask.
- Does the policy include coverage for ransomware negotiation and ransomware payment and if so, how much?
- Does the policy include coverage for data restoration and if so, how much? This question is obviously relative to the importance of and amount of data a company might have, and the risk associated with losing that data.

- Does the policy include legal services related to data privacy laws and disclosure requirements
- Does the policy include coverage for public relations services to reduce the impact of the incident on reputation risk?
- Does the policy include coverage for credit monitoring for individuals who are impacted due to disclosure of personally identifiable information?
- Does the policy include coverage for replacement or rebuild of hardware and key IT systems in the event a "scorched earth" approach is recommended for remediation?

Even after a thorough analysis of risks, appetite for risk, and difference in coverage relative to premium, many businesses still struggle to figure out how much cyber insurance is enough. It may be useful to consider the likelihood of having to deal with a cybercrime event relative to the other business risks for which a company traditionally purchases insurance. Consider the cyber insurance premiums and likelihood of experiencing a claim relative to general liability insurance, directors & officers, errors & omissions, and employment liability. This context may aid in deciding how much cyber insurance to carry.

Go West IT is routinely engaged for the first time by businesses who are experiencing a cyber incident. When cyber insurance is available, it is common to see the cost of even a small cyber event quickly go from $50,000 - $200,000. The forensic analysis firms and attorneys who specialize in these types of incidents will routinely cost $300 - $800 per hour, per resource. Ransomware payments for even small events will range from $10,000 - $200,000. IT services for business resumption efforts may be measured in the hundreds of hours.

Summary

Cyber insurance is an important consideration for any business that relies on technology to deliver goods and services to its customers. As with all insurance, you cannot get it when you need it. You must act in advance. Dealing with a cyber incident can be an incredibly stressful, time consuming, and costly endeavor. Every business should take time to discuss cyber risk, analyze exposure, evaluate mitigation strategies, and act to avoid, mitigate, and transfer risk, accepting what risk remains.