Top 5 Reasons Businesses Fail to Address Cyber Risk & What to do about it

One can debate how much cyber risk a particular business has or does not have but every single business has cyber risk, most businesses know this. Still, most have chosen to accept cyber risk rather than taking action to reduce the risk. The top five reasons businesses do not reduce cyber risk are:

1. Businesses do not understand the threat landscape and therefore the amount of risk they have.
2. Businesses do not know how to reduce cyber risk.
3. Businesses do not want to or cannot spend the money to reduce cyber risk.
4. Implementing controls to reduce cyber risk can be inconvenient to end users and even customers.
5. Businesses lack leadership support for risk reduction strategies.

Most business leaders are aware of cyber dangers. The headlines are filled with stories of attacks and most people have worked with a business that experienced a cyber incident or know someone who has dealt with a cyber incident. Still, people assume that because it has not happened to them, it probably will not. This flawed logic results partly from human nature and partly from not understanding the cybercrime landscape.

Is your business failing to address cyber risk? This article seeks to expose common cyber risk reduction barriers by:

1. Describing the threat landscape
2. Identifying cyber risk reduction strategies
3. Debunking the cyber security cost barrier fallacy
4. Putting cyber control inconvenience into perspective
5. Making the case for leaders to support risk reduction initiatives.

The Threat Landscape

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.

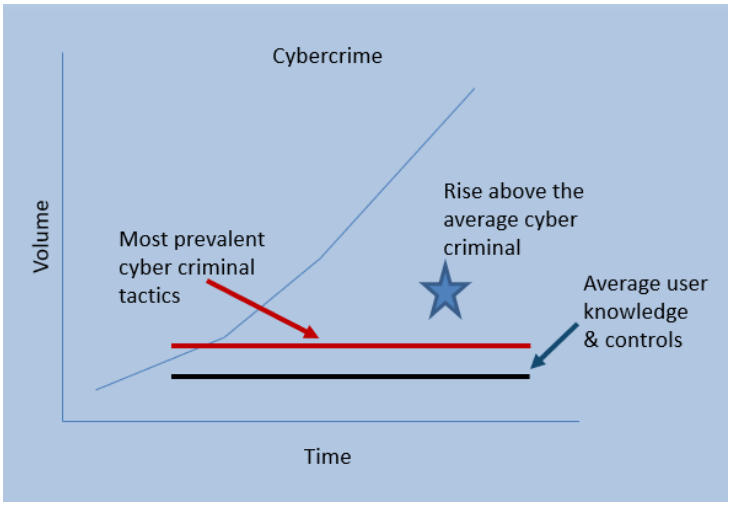
Cybercrime efficiency has resulted in increased risk for even the smallest businesses. Data ransom payments of $1,000 - $200,000 per event are very lucrative if accomplished efficiently by front line crime workers who use software as a service (SaaS) to deliver malware payloads, demand ransoms, collect payment, and send decryption keys. Personal data stolen from legitimate businesses is bought and sold on black markets for pennies per 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.

Risk Reduction Strategies

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, 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.

The Cost Barrier Fallacy

Many businesses do not take action to reduce cyber risk because they believe it will be too expensive. This is simply not true. Many of the actions a business should take to reduce cyber risk are inexpensive or even free. For example, enabling Multifactor Authentication (MFA) for email and most SaaS applications is usually free and only requires a small amount of configuration that can be accomplished by even the most technologically challenged user. Implementing MFA will significantly reduce risk.

As shown in Graph A above, a business may need only implement a small number of controls to substantially reduce the risk of falling victim to the most prevalent attacks.

It is true, comprehensive cyber risk mitigation strategies can be expensive, but this is changing. Cybersecurity solutions once available only to large businesses can now be acquired for relatively low fixed monthly fees based on the number of users or number of devices.

In many cases, acting is as simple as looking for a good managed security service provider that has bundled the software, hardware, and services necessary to mitigate risk. A managed service offering is a great way for a cost-conscious business to acquire solutions to reduce cyber risk. Let the IT security professionals do the hard work of choosing software, configuring solutions, monitoring alerts, and delivering a risk reduction outcome for a fixed monthly fee. This works equally well for businesses with an IT department and businesses that have no internal IT expertise.

Businesses that argue they cannot afford to deal with cyber risk are often the same businesses that cannot afford to survive a real cyberattack. The cost and inconvenience of reducing cyber risk is insignificant compared to the cost of dealing with a cyberattack. Businesses who have suffered a cyberattack will confirm this and are often willing to spend whatever it takes to avoid falling victim again.

Cybersecurity controls can be inconvenient, and inconvenience is relative

It is true, most, but not all cybersecurity risk mitigation strategies are accompanied by some degree of inconvenience. There is simply no way around this. However, we all make decisions about inconvenience vs. benefit every single day and when we accept inconvenience it is usually because the

alternative is potentially more inconvenient. This is true with the inconvenience of implementing cyber risk mitigation strategies.

The truth is that the inconvenience is relative an often not nearly as bad as people expect. Common inconveniences associated with cyber risk mitigation are:

- Multifactor Authentication prompts for accessing email, applications, file sharing, and VPNs.
- SPAM filtering solutions that sometimes classify legitimate email as SPAM.
- Creating, storing, and changing complex unique passwords.
- Having computer screens lock when not in use.
- Retrieving encrypted emails.
- Antivirus software or firewalls blocking access to websites.

The perceived inconvenience is often much worse than the actual inconvenience. Most end users adapt very well after a short adjustment period and before long the routine of working with new controls becomes second nature.

None of the admittedly inconvenient side effects of the above risk mitigation strategies come close to the impact of having all business data encrypted, having to tell customers that your business is unable to conduct business, having to pay a ransom to get your data back, or worse, telling customers that their data has been stolen. The impact of these real-life implications cannot be understated. In addition, the stress and mental toll experienced during a real cyberattack can be devastating. Victims of cybercrime report not sleeping for days on end, severe anxiety, a feeling of being victimized that is akin to experiencing a home break in, and incredible guilt.

Leaders must support cyber risk reduction initiatives.

Many businesses have not adequately reduced cyber risk to a level that is acceptable to leadership because leadership has not identified what risk is acceptable and committed resources and support to mitigate risk to an acceptable level. The irony of this reality is thick. Business leaders fall short in this regard because they fail to understand the risks, fail to ask for and listen to risk mitigation strategies, fail to commit time and resources necessary to reduce risk, and most importantly to explain why risk mitigation is important so that employees will accept the relatively minor inconvenience that may come along with risk mitigation strategies. Ultimately, leaders fail to lead when it comes to cyber risk mitigation.

This dynamic is changing. Shareholders, regulatory agencies, customers, and even managers are asking the "what if" questions about cyber risk and demanding that leaders grapple with this topic. Leaders of businesses need not be IT experts, but they can approach cyber risk as they do most other business risk by asking questions, weighing options, making decisions, setting a course of action, and supporting the work and effort of those asked to achieve the objectives.

There is no better time than the present to start discussions about a cyber risk mitigation strategy for your business. Assess, act, review, and repeat. Every step your business takes to reduce risk may be the step that saves your business.