Cyber Security

Developing a Strategy

Simple Mistakes / BIG Problems

A WHITE PAPER PRESENTED BY:

KG Hawes

Partners in Technology

2020

CONNECT: 1.866.687.9006 | kghawes.com | contact@kghawes.com

ABSTRACT

US Businesses are under constant assault.
66% of all small businesses worldwide experienced a cyberattack in 2019, with 76% of those based in the U.S. (1)

Cyber-security attacks have left businesses of all sizes holding their collective breath while scrambling to secure their IT systems. In the age of Covid-19, when a large sector of the workforce has been forced to work from home, often using unsecured devices, the forecast for 2020 looks exponentially risky for businesses, and full of opportunity for cybercriminals.

Though not immune from cyberattacks, large corporations typically have technical teams in place to monitor their systems: *entire departments focused on cyber security which can address issues as they arise and are equipped to handle breaches as they occur*. (2) Small businesses often lack the resources to implement that kind of strategy. That does not mean small businesses are without hope. A significant percentage of security issues are derived directly from user error. Often the first line of defense is for businesses to become educated on cybercrimes from the top down. Studies have shown that a lack of knowledge on the part of organizations and personnel are to blame for the majority of cyber security breaches, meaning that billions of dollars in recovery costs could have been easily avoided. Without proper education on cyber threats, businesses face increased liability for damage to their operating systems, their professional reputations, and to any customers, patients and employees a breach may affect.

As technology becomes more sophisticated, so do the quality and complexities of cyberattacks. From the smallest to the largest of companies, businesses should take nothing for granted – most especially their cyber security. Knowledge is truly power, and this White Paper focuses on the absolute basics. It is a failure to adhere to these simplest of preventative measures which will result in creating more than 90% of the vulnerabilities that hackers will be able to exploit.

Contents

No Business is Exempt

BIG Problems for Small Businesses

Recently, the *Congressional House Committee on Small Business* addressed the issue of cybercrime. Committee chairwoman, Renee Ellmers, began the session by citing a report from the Office of the National Counterintelligence Executive which showed billions of dollars are stolen every year through cyber means by foreign nations. She further stated that America's position as a wealthy nation and world leader in intellectual property meant our small businesses would inevitably remain "a primary target" for such criminals. (3) Many small businesses mistakenly assume cybercriminals are more interested in companies with larger assets. The truth is, more often than not, larger companies budget for security measures, whereas smaller businesses do not – making them easier prey.

A recent study stated that 44% of all cybercriminal activity focused on businesses with less than 400 employees. (3) Unfortunately, many of these businesses, which didn't have the resources to guard themselves from cyber threats in the first place, also didn't have the resources to recover from the attack, forcing them to close their doors.

"Cybercrime is the greatest threat to every company in the world."

IBM's president, Ginni Rometty, stated "Cybercrime is the greatest threat to every company in the world". (4) Many attacks could have been easily averted had the companies been properly prepared. Large corporations typically have technical teams in place to monitor their systems: *entire departments* focused on cyber security which can address issues as they arise and are equipped to handle breaches as they occur. Small businesses often lack the resources to implement that kind of strategy. (2) That does not mean small businesses are without hope. A large percentage of security issues are derived directly from user error and simple ignorance. Often the first line of defense is for businesses to become educated on cybercrimes from the top down.

Simple Mistakes Impact Large Corporations

In spite of spending millions of dollars annually on cyber security, large corporations are not immune to cyberattacks. In fact, given the significant payload potential offered by such breaches, large companies have become an increasingly popular target of cyber criminals over the last several years, including:

2019 AMCA, Citrix Systems, Capital One, Facebook, First American
2018 Marriott, MyFitnessPal, TicketFly, Google, Facebook
2017 Equifax, Uber, Yahoo, Deep Root Analytics, U.S. Universities
2016 Yahoo, U.S. Dept. of Justice, Tesco Bank, DNC, Apple
2015 Voter Registration Data, Anthem, Securus, Ashley Madison, T-Mobile

In *each* case, up to millions of sensitive data records were compromised, and in the end, upwards of billions of dollars in fines, fees and damages were paid out to affected consumers, patients and employees.

Lax Accountability and Weak Professional Standards

Though the *Deloitte* breach happened a few years ago in 2017, it will go down in cyber history as being one of the most egregious incidents of sloppy security, and is worth the repeated mention in this White Paper as a warning to other companies that regularly tout the tightest of IT security standards.

In September of 2017, less than a week after the UK multinational consultancy firm, Deloitte, shared a $593 million profit pool among its partners, it was hit by a cyberattack that enabled hackers to access usernames, passwords and personal information. Given that Deloitte provides high-end cyber security advice to some of the world's largest banks, companies and government agencies, this was quite an embarrassment and a hard fall from grace for a company consistently ranked by *Gartner* as "The Best Cyber Security Consultancy in the World." (16) After conducting his own open-source research shortly after the Deloitte breach, security researcher and founder of Phobos Group, Dan Tentler, stated "We're talking dozens of business units around the planet with dozens of IT departments showing very different aptitude levels. The phrase 'truly exploitable' comes to mind." (5)

Tentler questioned the security industry's ability to develop field-knowledgeable security professionals (read our White Paper on "The IT Shortage"). He stated that the bigger problem facing companies was a culture of what he considers "smoke and mirrors" in information security with lax accountability and weak professional standards. "The security industry is sick" and incidents like the one at Deloitte are just symptoms of that sickness. (5)

Understanding the Threats

The first step in protecting your business from cyber threats is to understand what kinds of threats exist. Many potential attacks can be easily averted if the risks can be identified. It is of the utmost importance that all managers, even the non-tech savvy, have an understanding of how cyber security works – In turn, it is their job to educate and monitor their staff. Understanding the fundamentals of cyber security attacks is beneficial for all employee levels. The following is a breakdown of the most common forms of cyber security threats and how they function within your system.

Malicious Software (Malware)

There are many different forms of malware. Malware is defined as "any" software which is designed to damage or debilitate a computer or computer system. The following is a brief breakdown of the primary forms of malware.

Viruses

Viruses are either programs or codes that attach themselves to benign applications and then replicate when the application is activated, thus "infecting" the new computer system in the same way one would contract the common cold. Viruses can take the form of harmless annoyances, often used as "pranks," and others are malicious acts designed to steal confidential information or sabotage functionality.

> One of the most famous viruses to date duped its victims by resembling a friendly email message. The virus, dubbed the "Love Bug" appeared as an email with ❤ "I Love you" written in the subject line and was hidden in what looked like a harmless text file. When a user opened the message, the virus worked its way through the system overwriting files at random. The "Love Bug" also sent itself to every address saved in its victim's email account. This made the email appear more legitimate as it came from an acquaintance's email address. By the time the virus was discovered, it had claimed tens of millions of victims.

Worms

Worms are similar to viruses in that they have the ability to replicate themselves; however, they function differently. They are designed to spread through computer networks without the necessity of an application to act as a host. Worms have the potential to enact damage on a system in a variety of ways, whether simply absorbing bandwidth or selectively consuming data or operating system files.

Trojan Horses

Trojans are also self-replicating but unlike worms or viruses they are standalone applications written to look like something else for the purpose of being used as an attack tool. A Trojan fools the user into thinking it is an authentic program then it's downloaded and installed by the user's own volition. Trojans are designed to give a hacker remote access to your system controls and data.

Backdoors

Backdoors are essentially hidden entry points created to give hackers VIP access to your system. Backdoors bypass standard security measures and can give someone access to a business's entire network allowing them to install or modify nearly anything they wish.

Rootkits

Rootkits provide attackers with continued access to systems already infected by malicious software. This kind of malware is very difficult to detect by nature and can fool anti-virus software into overlooking an open breach. Rootkits do not contain code that is harmful to your system on its own; the danger lies in their ability to become a tool for hiding the existence of other malware.

Keyloggers

Keyloggers provide a record for cyber-criminals of everything the user types. They can be installed on a system in conjunction with, or as a part of, another malware program like a Trojan horse or Worm. Keylogging can be an effective strategy to capture passwords and credit card information. Most typical anti-virus software is incapable of detecting keyloggers.

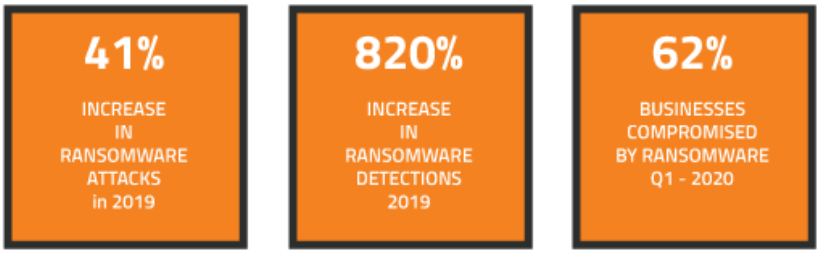
Spyware and Adware

These forms of malware often work together. Spyware acts to track and record a user's activities. This could be used to collect an infinite amount of confidential information. Most commonly, Spyware is used to track a user's internet activity and enable the appropriate adware. Adware displays unwanted advertisements. While Adware may seem somewhat harmless, if left unchecked it can severely impair processing speeds.

Ransomware

Ransomware is a cyber version of extortion. The malware typically locks a system down making it impossible to access until the user pays a "ransom" for its release. Ransomware is usually disguised as a legitimate error message, or application which the user unintentionally activates (7). In past years, the practice of creating regular backups would allow victimized companies to ignore the ransom demands of an attack; however, in 2019, ransomware groups circumvented this by creating a copy of a company's sensitive data and threatening to publish it online if the ransom wasn't paid. 2020 also saw a surge in coordination amongst ransomware attacking gangs. (17)

Ransomware Statistics *for* **2020**



(Information source: (8))

More Threats in a Cyber-Criminal's Toolkit

Following are some of the other strategies cyber-criminals employ for invading a system or network:

Hijacking or Man-in-the-Middle Attacks

Hijacking, sometimes referred to as a man-in-the-middle attack, occurs when a hacker "hijacks" communication between two parties. Positioning themselves as the middle man allows criminals to intercept information and in some cases, impersonate one or both of the parties to obtain usable information such as user names or encryption keys.

Spoofing

In a spoofing attack, cybercriminals obtain unauthorized access to a system or network by presenting fraudulent identification. There are several versions of spoofing such as email, caller ID and URL. A common form which affects businesses, occurs when the attacker mimics an approved IP address to sneak through an existing security filter.

Packet Sniffing

Packet sniffing is a way to capture data being passed through your network. Packet sniffing is enacted by a specialized application (or sometimes hardware devices) that intercept the "packets" that move information back and forth. The intercepted information is logged, decoded then scanned for valuable content according to the specifications in which the "sniffer" was built.

Unfortunately, a lot of the data that is moved across business networks is left unencrypted leaving it vulnerable and exposing confidential data or passwords. In some cases, this information can be used to duplicate or change previously taken actions, such as bank transactions.

DDoS

Distributed denial of Service (DDoS) refers to attacks where the user's access is compromised. This is typically achieved by overwhelming the computer so that it cannot process the user's

requests. Network access can be disrupted in the same way. Between Q3 of 2019 & Q1 of 2020, DDoS attacks increased by 542%.

> Researchers attribute the sharp rise in DDoS attacks "…to malicious efforts during the COVID-19 pandemic when most consumers became dependent on online services while workers started working from home during the pandemic to prevent the spread of the virus. The heavy reliance on remote services overwhelmed most ISPs thus allowing the attacks to take place." (10)

Port Scanning

A "port" is essentially a connection point for communication within your operating system. Port scanning is a strategy employed by hackers to find exploitable vulnerabilities in network services. An open port on a computer system is essentially an open door, allowing the attacker to enter through the network, steal information, plant malware, or even render the system useless.

Password Cracking

Using a password is the easiest way for hackers to get access to confidential accounts and information. Cracking passwords can be achieved through a number of methods whether simply guessing or using elaborate programs that test infinite password possibilities at accelerated rates. Improperly managed and poorly constructed passwords have held the number one rank for sources of cyber security breaches for over thirty years. (15)

Improperly managed and poorly constructed passwords have held the number one rank for sources of cyber security breaches for over thirty years. (15)

Phishing

> "A single spear-phishing email carrying a slightly altered malware can bypass multi-million dollar enterprise security solutions if an adversary deceives a cyber-hygenically apathetic employee into opening the attachment or clicking a malicious link and thereby compromising the entire network."
>
> - **James Scott, Senior Fellow, Institute for Critical Intrastructure Technoloy** (6)

Phishing is one of the most dangerous and most common ways cybercriminals violate a system. In this approach, the hacker "baits" the user by imitating a trustworthy site or business via email or the internet. In these attacks, the user is fooled into supplying the criminal with the desired information. Impersonations of banking, shopping or social media sites are common. Phishing is also sometimes used to redirect the user to a site containing malware. For a business, phishing is a malicious threat – All it takes is one employee falling prey to the phishing scam to infect the entire network. One of the biggest data breaches experienced by the financial paragon J.P. Morgan wasn't achieved by hackers' elaborate programming but rather employees falling for phishing scams. (11)

> **78%** of users admit to being aware of the risks of unknown links in email-phishing scams but click on them anyway. (12)

Structured Query Language (SQL) Injection

One of the oldest and most popular hacking techniques, SQL Injection attacks target databases by "injecting" malicious code into the language used for managing the data. Hackers can then access or alter sensitive data (such as a process) for other purposes like identity theft and fraud.

Ignorance is Risk – The Human Factor

Most cyber security threats rely upon ignorance and could be easily prevented by an informed user. For businesses, computer system and network vulnerabilities typically occur when employees use them incorrectly or fail to recognize problematic issues. There are many ways in which risky behaviors can be addressed to negate the likelihood of making your business a target. The following section will outline potential vulnerabilities in a system or network, with an eye on the biggest: **The Human Factor**.

Weak Authentication

Authentication is the way in which your system verifies the authorization of a user. There are multiple ways authentication processes can be applied. The most common way is the use of a password or security questions. More complex forms of authentication are becoming common, such as the finger print or facial recognition that is being experimented with in new smart phone technology. It is probably not surprising that requiring multiple forms of authentication is the best way to prevent vulnerabilities in this area. Businesses should consider implementing multi-factor authentications where confidentiality and the protection of assets is a top priority.

As of December 2019, **71%** of user accounts are protected by passwords that are used on multiple websites, in spite of the fact that a whopping **90%** of all users are worried about getting their passwords hacked; while, **57%** of those who have been scammed on phishing attacks still haven't changed their passwords. (13)

Keys and Certificates

Keys and certificates are essentially electronic credentials. Keys and certificates work together in an authentication process to ensure that only the intended users can decrypt a message or file. Keys can either be "public" or "private." A "private" key is possessed only by the originators while "public" keys get distributed to receivers. Certificates are used to prove ownership of keys. Unprotected keys and certificates can be abused by hackers. If stolen, they can be used for a variety of purposes, like spying or sabotaging, as well as disguising malware as something legitimate. **Over 50% of businesses do not know where to find their keys or certificates, who is responsible for them, or how they are used**. (12)

Patches and Updates

Patches and updates fix issues discovered in previously installed software or applications. Staying on top of current patches or updates for your company's systems both improves performance and negates potential weaknesses that could be exploited. 60% of breaches involved vulnerabilities for which a patch was available but not applied. (9)

Encryption

Encryption conceals your data to protect it from easily being seen or used by non-authorized users. The encryption process uses an algorithm to encode data and provides a user specific key to decipher it. For many businesses, encrypting data is mandatory for compliance reasons. Improper encryption practices can provide needless opportunities for cybercriminals to exploit.

"Good Hygiene" Stops 75% of Cyber Threats

"I would say two things, and they are really the central recommendations of our task force. Number one is what is called good hygiene. It is the basic things that we all know we should do but too often don't do, keeping our firewalls up to date, our virus protection up to date, not having our passwords underneath our mouse pads in our offices…the task force received information from a variety of witnesses saying roughly three-fourths of the malicious stuff out there on the Internet could be stopped if we all did the basic stuff we know we are supposed to do. So, small businesses, you know, it doesn't take a lot of money, but you need to do the stuff you know you should do."

(Source: US Representative Thornberry. Hearing before the Committee on Small Business. April 20th 2016.)

The Cost of Recovery

The recovery cost for a business after a cyber-security breach is far beyond a simple monetary problem. The damage incurred is often multi-faceted.

Sources for recovery costs which must be considered are:

- Loss of assets
- Regulatory costs and compliance fines
- Intellectual property theft
- Operational performance
- Shareholder value
- Litigation expenses
- Revenue during a temporary shut-down
- Data and system recovery services
- Brand & reputational harm
- Lost customers

Cyber Crime Harm Matrix			
Harm Type	**People**	**Processes**	**Technology**
Financial Loss	Job Security	Loss of Efficiency	Cost of Replacement
Denial of Service	Ability to Work	Loss of Services	Loss of Access
Customer Experience	Customer Relations	Customer Care Costs	Site or Call Traffic
Data Breach	Fraud Losses	Audit & Investigations	Suspension of Use
Employee Trust	Confidence & Morale	Productivity	System Access
Brand & Reputation	Confidence & Morale	Marketing Costs	Trust in Systems

(Information source: *Cyber Crime, Security and Digital Intelligence*.)

In 2019, it took an average of 287 days, at a cost of $7.5 billion, for a business to recover from a cyber-attack. (8) The compounding of these cost factors is the reason why many small

businesses are left with no alternative to closure. The actual cost of recovery for your business is as impossible to predict as the cyberattack that could trigger it. Statistics for cyber-related crime costs to businesses worldwide are increasing yearly, at a staggering rate.

Developing a Strategy for Cyber Security

The best way to protect your business is to develop a strategy for cyber security. Educating management and staff is a good first step but **a complete strategy will include an assessment of your cyber infrastructure and the implementation of security policies.** Your strategy should be a *continuous process*; regularly evaluating security controls, modifying systems with up-to-date patches and encryption methods, and staying apprised of the latest scams and threats.

Cornerstones for Cyber Security Strategies

Detection Systems

Some kind of Intrusion Detection System (IDS) should be in place. These take the form of either hardware devices or software applications. When potentially malicious activity is detected, the IDS sends a report to an administrator or security management system for analysis. Some of these systems have an integrated ability to address and prevent intrusions.

Multi-level Security

A technique referred to as multi-level security can be applied to manage sensitive data. In this process, data is categorized by sensitivity level and access is parceled out on a need-to-know basis. Implementing a hierarchy for data within your system can limit availability of your most important data, making it more difficult for hackers to view and steal as well as prevent confidential information from accidently being accessed by the general population of employees.

Firewalls

A firewall is crucial to network security because it monitors the traffic and acts as a barricade against traffic from unverified sources. Firewalls can be either software or hardware based and more than one firewall can be implemented at a time. For this reason, firewalls are often a front line of defense against cyber breaches.

Antivirus software

Antivirus software can not only prevent viral attacks, it can also detect and remove the malware. Over the years, antivirus software has become more robust and effective in preventing common malware attacks like Trojan horses and rootkits. Having current antivirus software offers an additional layer of protection with its ability to immediately detect and notify the user in the instance of a “human-factor” mistake.

Smart Authentication Practices

Implementing a strategy for password creation and use is an effective first step. Password policies should be specific about length and character usage as well as include regular expirations to prevent the "one password for everything" habit most employees fall into. A password blacklist should be distributed and included in the policy to prevent the use of atypical passwords known to be insecure. Developing multi-factor authentication practices, as discussed previously, can guard your business against any number of preventable intrusions and are more secure than passwords alone.

Secure Data Management

Your business's data management should be addressed specifically in addition to other security measures. Having a secure encryption strategy and access controls are essential in ensuring the confidentiality of your data. There are many software solutions for data management which include precautionary security controls.

> 81% of data breach victims reported that they neither had a system nor security service in place to ensure they could self-detect breaches. (14)

Summary

The education of your company's supervisors and front-line staff is an essential step in preventing cyber security breaches. With the continued development of technology and tools come new threats and opportunities for cyber criminals. Regular auditing is the only way to accurately assess the risk for your business. Since the realm of cybercrime is so vast, you want to leave no virtual stone unturned. For your business, developing a strategy and practicing "good hygiene" could be the difference between realizing potential and becoming another failure in the headlines.

What KG Hawes Offers

KG Hawes offers a variety of services to help businesses with their cyber security needs. Our low-cost, no-obligation cyber security assessment will provide you with information needed to accurately gauge your business' state of risk. Our pre-assessment audit includes an inventory of your existing system's security and a vulnerability analysis. We take pride in offering affordable solutions and will apply the cost of your pre-assessment to any full audit services you request from us. KG Hawes builds lasting relationships with our client's through exceptional service, which is why we offer our client's customized solutions and 24-hour support.

KG Hawes uses the Common Vulnerability Scoring System (CVSS) to identify and prioritize vulnerabilities in computer security system audits. CVSS scores evaluate potential vulnerabilities based on the ease and impact of the potential exploit on a scale of 1-10. The CVSS evaluation focuses on three metrics; base, temporal and environmental. The combined metrics of this scoring system give a clear overall impression of the severity of a system weakness which is why security auditing should be a regular component of any businesss' security strategy.

Pre-Assessment Audit

Inventory
Assess Risk Inventory
Perform Automated & Manual Vulnerability Analysis
Perform and Check Security Misconfigurations
Perform Patch Audit for Software & Operating System in Network

Firewall Audit
Perform Audit on Misconfigurations
Firewall Base Rule Test
Internal DDOS Test

Web Application Audit
Audit Webservers for Security Issues
Audit External Facing Web Application Security Audit
Audit Web Application for Default & A1 Injection

Network
Perform Software Patch Audit
Perform Router Misconfiguration Audit
Perform Antivirus and Malware Audit
Perform DNS Audit
Perform Internal Misconfiguration Audit

SIP Audit
Perform SIP Audit
Perform Vulnerability Analysis

References

1) Osborne, C. (2019, October 08). 76% of US businesses have experience a cyber attack in the last year. Retrieved August 19, 2020, from https://www.zdnet.com/article/76-percent-of-us-businesses-have-experienced-a-cyberattack-in-the-past-year/
2) Vomiero, J. (2017, June 30). Small businesses often more vulnerable to cyberattacks, experts say. Retrieved October 23, 2017, from https://globalnews.ca/news/3567122/petya-ransomware-cybersecurity-businesses/
3) N/A. (2019, October 23). 10% of Small Businesses Breached Shut Down in 2019. Retrieved August 20, 2020, from: https://www.darkreading.com/operations/10--of-small-businesses-breached-shut-down-in-2019/d/d-id/1336156
4) Morgan, S. (2015, November 24). IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'. Retrieved October 23, 2017, from https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#1e59a48073f0
5) Paul. (2017, October 02). Hacker Eye on the Consultant Guy: Deloitte and the Art of spotting Vulnerable Firms from the Outside. Retrieved October 23, 2017, from https://securityledger.com/2017/10/podcast-hacker-eye-consulting-guy-deloitte-hack/
6) Scott, J. (Date Unknown). Quote. Retrieved on: August 20,2020, from https://www.goodreads.com/quotes/tag/phishing
7) Unknown. (2017, April). 2017 Internet Security Threat Report. Retrieved October 23, 2017, from https://www.symantec.com/security-center/threat-report
8) Unknown. (2020, February 27). 20 Ransomware Statistics You're Powerless to Resist Reading. Retrieved August 20, 2020, from: https://www.thesslstore.com/blog/ransomware-statistics/
9) Frulinger, J. (2020, March 9). Top cybersecurity facts, figures and statistics for 2020. Retrieved August 20, 2020, from https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
10) Hope, A. (July 10, 2020). Report Says DDoS Attacks Increased by Over 500% Because of Covid-19 Pandemic. Retrieved August 20, 2020 from: https://www.cpomagazine.com/cyber-security/report-says-ddos-attacks-increased-by-over-500-because-of-the-covid-19-pandemic/
11) Green, J. (2016). Cyber security an introduction for non-technical managers. London ; New York: Routledge.
12) Kramer, A. (2017, June 09). 35 cyber security statistics every CIO should know in 2017. Retrieved October 23, 2017, from http://etsconnect.com/35-cyber-security-statistics-every-cio-know-2017/
13) Arzina, L. (2019, November 19). Password statistics for 2020 – 'iloveyou' and 'sunshine' are most common. Retrieved August 19, 2020, from https://dataprot.net/statistics/password-statistics/
14) Acito, D. (1970, May 01). 15) 8 Ways Businesses are Vulnerable to Cyber Attacks. . Retrieved October 23, 2017, from http://it.toolbox.com/blogs/hardware-tech-windows/8-ways-businesses-are-vulnerable-to-cyber-attacks-76325
15) Acito, D. (1970, May 01). 15) 8 Ways Businesses are Vulnerable to Cyber Attacks. . Retrieved October 23, 2017, from http://it.toolbox.com/blogs/hardware-tech-windows/8-ways-businesses-are-vulnerable-to-cyber-attacks-76325
16) Gartner. (2013, July 25). Deloitte ranked #1 in global consulting [Press release]. Retrieved October 23, 2017, from 16) https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-ranked1-global-consulting-gartner.html
17) Bison, D. (2020, August 4). Security Intelligence. 6 Ransomware Trends You Should Look out for in 2020. Retrieved August 20, 2020, from: https://securityintelligence.com/articles/6-ransomware-trends-2020/