The Burnie Group

UNDERSTANDING CYBERSECURITY

INSIGHT REPORT on Cybersecurity
prepared by The Burnie Group

DECEMBER 2017

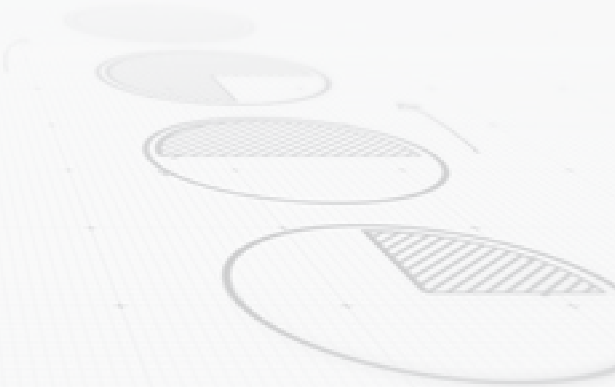
WHAT IS CYBERSECURITY?

Cybersecurity, at its core, is the protection of data against unauthorized and criminal use. It is the only defense in the real-life digital war being waged between hackers and businesses.

The basic elements of cybersecurity, developed by the US Commerce Department's National Institute of Standards and Technology (NIST), include:

1. Identifying critical systems;
2. Protecting systems by implementing strategies to safeguard the delivery of services;
3. Detecting threatening events in a timely manner;
4. Responding to the event through strategic action;
5. Recovering impaired capabilities and services so normal operation may resume.

As technology advances, so do ways of exploiting and attacking these new advances. Attacks on businesses increased 300% in 2016[1] and are expected to cost businesses $6 trillion annually by 2021[2]. Cybersecurity measures must continue to advance in order to mitigate the ever-growing threat.



[1] https://www.justice.gov/criminal-ccips/file/872771/download

[2] https://cybersecurityventures.com/hackerpocalypse-original-cybercrime-report-2016/

HOW IS CYBERSECURITY THREATENED?

Cybersecurity threats come in many forms and are continuously mutating. At the same time, public awareness of the problem is increasing. Several of the largest cybercrimes on record occurred within the last year.

Data theft: In September of 2017, Equifax publicly admitted to one of the biggest data breaches in history. Over several months, hackers had gained access to the private information of 145.5 million American customers, up to 44 million UK customers, and 100,000 Canadian customers. The stolen information included names, addresses, driver license numbers, Social Security numbers, and credit card numbers. Equifax shares dropped 13% within a day of the announcement, and numerous lawsuits have since been filed.

Fraud: The "Nigerian Prince" scam is one of the best known digital fraud scams of all time. Fraud scams are simple: convince someone that they have won something, that a family member is in need, etc. Victims that don't recognize the scam voluntarily hand money over to their attackers. Hackers are continually altering their methods, graduating from phishing emails to hacks of social media accounts, which they use to impersonate individuals and extort money from family and friends. Despite the widespread knowledge of these scams, it was estimated that in 2013 Nigerian scams netted $12.3 billion[3].

Denial of Services: This style of attack involves taking a machine or network hostage by overloading it with superfluous requests, temporarily or indefinitely disrupting the services it offers. In October of 2016, a DoS attack took several major sites hostage, including Twitter and Amazon. The motivation for this type of attack isn't always clear, as it typically does not involve theft of information. A DoS attack is used more often as a mobster-style threat: pay us protection money or we will take your site. It can also be used as a smoke screen, to distract an IT team while the real cyber crime takes place.

Political Attacks: The threat of cyberattacks increases as hackers graduate from individuals to businesses, to entire governments. Famously, WikiLeaks released thousands of pilfered Democratic National Committee emails that rocked the 2016 presidential election. More recently, two days before the French election, hackers released a trove of stolen e-mails from the party of Emmanuel Macron, with the goal of influencing the election.

Ransomware: Ransomware is the most prevalent and profitable type of cybercrime. Global ransomware damages are projected to exceed $5 billion by the end of 2017[4]. May 2017 saw largest and most devastating ransomware attack ever: WannaCry. This attack demonstrated a new form of cyber threat. It used no tricks, no phishing-emails, no exploit kits. Instead, it used an existing software vulnerability in Windows operating systems that had been previously identified by the U.S. National Security Agency. Within hours, it spread across industries and borders, infecting computers in over 150 countries. It took data hostage, demanding ransom for its return. The situation devastated the UK's National Health Service and affected universities, airports, and production for hundreds of companies across the world. Damages from WannaCry's ruthless takeover are estimated to be about $1 billion.

[3] https://www.geektime.com/2014/07/21/millions-of-victims-lost-12-7b-last-year-falling-for-nigerian-scams/

[4] https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

HOW DOES CYBERSECURITY WORK?

Cybersecurity is structured like an onion, involving layers upon layers of varying degrees of security. Multiple security levels are required to ensure data is accessed only by authorized personnel or processes. Strong cybersecurity goes beyond good password management or use of firewalls to prevent access. These security measures may include:

Audit logs: allows system activity to be tracked to identify the source and extent of any breach. The preservation of the integrity of audit logs is an important consideration as hackers will try to erase or alter logs in order to hide their activity.

Encryption: ensures data can only be accessed by an individual with the proper encryption key.

Access control: used to manage accounts, record log-in attempts, and enforce access policy.

Data Loss Prevention: protects against unauthorized access by preventing data from being sent outside of a network.

Intrusion Detection System: detects ongoing attacks, and records activity to assist in the post-event investigation.

Security Information and Event Management: provides real-time analysis of security alerts.

HOW IS CYBERSECURITY CHANGING?

As technology evolves, threats evolve. Businesses are increasingly becoming more digitized and processes more automated. The proliferation of Internet of Things (IoT) devices and the increasing commonality of peer to peer interactions, is a growing cause of stress on cybersecurity protocols. Furthermore, the increase in diverse distributed ecosystems featuring high-degrees of automation will keep security experts busy as they try to keep up with rapidly evolving business requirements. As services, such as transportation, become digitized, the risk of terrorism through hacking becomes a serious cause for concern.

Blockchain technology is emerging as a powerful security mechanism to ensure logs are immutable and tamper-proof. The use of blockchain increases security for messaging, digital payments, and more. Blockchain plays an important role in securing value and currency flows, as well as allowing IoT devices to transact securely and confidently.

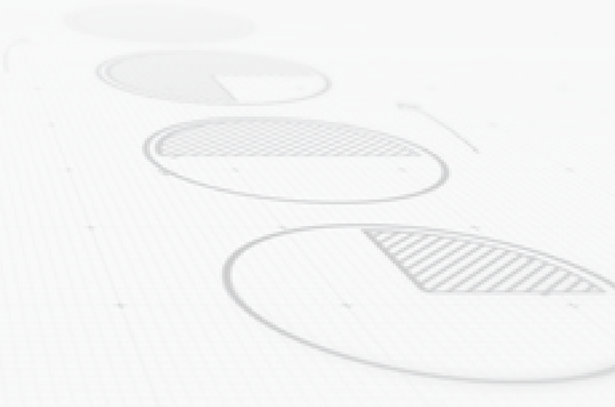
There is also great potential for the use of artificial intelligence (AI) in cybersecurity. Within a few years, AI-enhanced security programs will be able to patrol chat rooms and social media, using language processing to recognize potential cyber attacks before they happen. With the appropriate management of cybersecurity systems, the threat of attack can be greatly minimized.

THE FINAL WORD

Cyber attacks are a strong and real threat. In 2016, 71% of businesses attacked were successfully infected[5]. Assume you will be attacked at some point. Ensure you have a cybersecurity system in place to prepare for possible attacks, to protect you, your partner, and your client's interests, and to plan for the eventuality of responding to and investigating an attack.

Remember, you are only as strong as your weakest link. Your cybersecurity system must be kept up to date. Your security policy and procedures should be tested and stressed, and employees should be involved in regularly scheduled security policy and practices education. Keep in mind that, through 2020, 99% of the vulnerabilities exploited by cyber attackers will be ones that will have been known to IT professionals for at least one year[6]. Equifax knew as early as March of 2017 that their system was vulnerable, yet they failed to implement a simple patch for the issue[7]. The NSA had discovered the weakness in Windows' operating systems months before WannaCry, and yet did not inform Microsoft, choosing to exploit the flaw themselves.

With the proper cybersecurity in place, you can be ready to deal with any attack, or fatal flaw, that comes your way.



[5] https://blog.barkly.com/cyber-attack-statistics-2016

[6] https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/

[7] https://gizmodo.com/equifax-was-warned-about-vulnerability-but-failed-to-pa-1819065186

● The Burnie Group

The Burnie Group is an experienced management consulting firm that helps clients design innovative strategies and continuously pursue operations excellence.