Cybersecurity

What is Cybersecurity?

Cybersecurity is the technology, processes, and practices that protect networks, devices, programs, and data from cyberattacks, damage, or unauthorized access [1]. Cyberattacks are an evolving danger to organizations, employees, and consumers, as they can access or destroy information, or even extort money. They have the ability to destroy businesses and damage people's financial, and personal, lives [2], and a career in cybersecurity means working to make sure that doesn't happen.

As our world becomes more tech-focused, organizations and people store unprecedented amounts of data on their devices (photographs, passwords, banking information and more), so cybersecurity is becoming increasingly important!

Cyberattacks are a constantly growing, and evolving. Cyber criminals find holes in coding and new ways to exploit networks, so we all need to be prepared with excellent cybersecurity.

digital nova scotia

Cybersecurity Threats

There are many types of cyberthreats that can attack devices and networks, but they generally fall into three categories [3]:

Attacks on Confidentiality - these include stealing personal identifying information, and bank account or credit card information. Many attackers will take individuals information and sell it on the dark web for others to purchase and use.

Attacks on Integrity - these attacks consist of personal or enterprise sabotage, and are often called leaks. A cybercriminal will access and release, sensitive information for the purpose of exposing the data, and influencing the public to lose trust in that organization.

Attacks on Availability - the aim of this type of cyberattack is to block users from accessing their own data until they pay a fee, or ransom. Typically, a cybercriminal will infiltrate a network and block access to important data, demanding a ransom to release control. Companies sometimes pay the ransom and fix the cyber vulnerability afterward so that they can avoid halting business activities.

Careers in Cybersecurity

Due to the constant evolution of cyberattacks and creativity of cybercriminals, there is always an industry need for trained professionals who understand how best to prevent cyberattacks. Some of the most common professions in this industry include [4]:

Security Analyst: This role analyzes and assess' vulnerabilities in the infrastructure (software, hardware, networks), investigates available tools, or countermeasures to remedy any detected vulnerabilities, and recommends solutions. A security analyst also analyzes and assesses damage to the data/infrastructure as a result of security incidents. They might also assist in the creation, implementation, and management of security solutions.

Security Engineer: Performs security monitoring, security and data/logs analysis, and forensic analysis, to detect security incidents and response to them. A security engineer also investigates, and utilizes, new technologies and processes to enhance security capabilities and implement improvements.

Security Architect: Designs a security system or major components of a security system, and may head a security design team building a new security system.

Security Software Developer: Develops security software, which includes tools for monitoring, traffic analysis, intrusion detection, virus/spyware/malware detection, anti-virus software, etc. Also implements security into applications software.

Important Skills

As a cybersecurity professional who works as part of a broader team, other valuable skills that help are [5]:

- **Ability to work in a team environment, and collaborate with others**
- **Communications skills**
- **Organizational and problem-solving skills**
- **Integrity and discretion**

Skills that Help Professionals

A few technical and functional skills, needed to work in cybersecurity are [6]:

Understanding of Security Principles: An understanding of basic security principles, such as privacy, confidentiality, authentication, access control, and others.

Malicious Codes: A working knowledge of malicious codes, which are any codes in a system that are intended to caused harm. They need to know how they are propagated, and the risks associated with each.

Risk Analysis: To be able to assess a client's particular security needs, which requires knowledge of risk analysis principles.

Intruder Techniques: In analyzing attacks, personnel should be able to recognize known intruder techniques, their characteristics and effects, and identify new intruder techniques by means of elimination of known ones.

Statistics About the Industry

According to Canada's Information and Communications Technology Council's Digital Talent Outlook, a cybersecurity analyst will be one of the most in-demand jobs in the tech sector of Canada between now and 2023 [7].

The average salary for any position in the cybersecurity field (analysts, engineer, etc.) varies greatly, as it is between $44,000-$105,000 in Canada, depending on what job you're working, experience level, location, employer, and education towards the specific field [8].

In 2018, Canadian police services reported that there were almost 33,000 cyber-related crimes, which was a 12 per cent increase from the previous year [9].

Where to Get Started?

With cybersecurity becoming more in demand across almost all industries, now is a great time to enter the industry. There are several post-secondary courses in Nova Scotia for students to enroll in, that will give them the skills and knowledge to be working in cybersecurity:

Nova Scotia Community College (NSCC) Cyber Security [10]: In this program, students will learn how to provide the information, and tools, necessary to identify and secure potential vulnerabilities. Students explore a variety of information and system security areas and methods, including ethical hacking techniques, risk analysis, cryptography, vulnerability testing, auditing, and security management.

Nova Scotia Community College (NSCC) IT Systems Management and Security [11]: In this program, students design the implementation and management of the core technologies that support information communication technology (ICT). These technologies include UNIX/Linux and Windows network operating systems, local area network (LAN) and wide area network (WAN), security implementations to protect data and users, and systems analysis and design (SAD).

Saint Mary's University (SMU) Computer Science [12]: Computer science involves the systematic study of the algorithms that underlie the acquisition, representation, processing, storage, communication of—and access to—information of all kinds. It also involves the study of computing platforms and programming languages, such as C++ and Java. In this program, students will explore creative ways to solve problems as they discover how computers and computer systems can be applied to everything from medicine, to security, to entertainment. Students will also develop other marketable skills, such as project management, and software design and development.

Dalhousie University Computer Science [13]: Students will gain a deep understanding of the theory, design, and application of computer science by exploring a wide range of areas including software development, algorithms, networking and graphics. In this program, students will gain the foundational knowledge to create new, and innovative, technologies that will shape how we use computers and how we interact with each other in the future. Students take courses that will expand their knowledge about operating systems, cybersecurity, machine learning and AI, and much more.

WHAT DO THE PROFESSIONALS THINK?

PHILLIP COUSINS

DIRECTOR - RISK AND SECURITY CONSULTANCY, RBC

Philip Cousins, the Director of Risk & Security Consultancy at RBC, has been working in cybersecurity for 20 years, and said demand for the profession has dramatically increased since he first entered the industry.

“The environment for cybercrime has grown massively over the years, as cyber attackers have become very organized and established. They can attack you in a variety of different ways – from defrauding accounts, spam hacks, ransomware, to many other methods of hacking. Due to this, most organizations have put an increased importance on hiring cybersecurity professionals to protect their information.”

Philip believes now is a good time for people to get into the profession due to the high demand, as well as that the pay rates are good compared to other jobs in tech. Also, there is less risk of this work being automated by machines in the future due to the complex, and specific, nature of the work.

He said the best advice he could give someone who is thinking about getting into cybersecurity is to do research about the profession.

“If you’re curious about cybersecurity, follow your interest learn as much as you can about it. Research some of the major data breaches that have happened, and read about how it happened, how they breached the system, and how they could have better defended it. Just keep following your curiosity.”

digital nova scotia

WHAT DO THE PROFESSIONALS THINK?

ROHID SHARMA

SALES DIRECTOR, CYBERCLAN

Rohid Sharma a Sales Director at CyberClan, and has been working in the industry for three years. He said cyber attacks have increased exponentially in volume since he first started.

“Cyber attacks have been more sophisticated and targeted over the years, as the price for data online has gone up tremendously.”

Rohid also talked about how the industry is doing in Nova Scotia, and said that currently, it’s a great time to be a cybersecurity professional in the province.

“Though businesses as a whole are still a little behind on their understanding of their need for cybersecurity, I’ve found that mindset is slowly changing. As a result, more businesses and government offices are starting to get more cyber-conscious, and are hiring people to protect their data. So, it’s a great time to be a cybersecurity professional in Halifax.”

When asked what advice he would give to students, Rohid simply encouraged them to keep an open mind.

“As businesses’ dependence for technology continues to increase, the need for cybersecurity professionals will also increase. There are quite a few cybersecurity professionals that work remotely in Nova Scotia for companies out of province, and I believe remote work will only continue to grow in popularity over the coming years.”

digital nova scotia

References page 3

[1] https://digitalguardian.com/blog/what-cyber-security
[2] https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html
[3] https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html
[4] https://www.cs.seas.gwu.edu/cybersecurity-roles-and-job-titles
[5] https://www.learnhowtobecome.org/computer-careers/cyber-security/
[6] https://www.learnhowtobecome.org/computer-careers/cyber-security/
[7] https://www.ictc-ctic.ca/wp-content/uploads/2019/11/canada-growth-currency-2019-FINAL-ENG.pdf
[8] https://www.glassdoor.ca/Salaries/canada-cyber-security-analyst-salary-SRCH_IL.0,6_IN3_KO7,29.htm
[9] https://www150.statcan.gc.ca/n1/pub/89-28-0001/2018001/article/00015-eng.htm
[10] https://www.nscc.ca/learning_programs/programs/plandescr.aspx?prg=CYBR&pln=CYBRSCUR
[11] https://www.nscc.ca/learning_programs/programs/PlanDescr.aspx?prg=ITSM&pln=ITSYSSEC
[12] https://smu.ca/academics/computing-science.html
[13] https://www.dal.ca/faculty/computerscience/undergraduate-programs/study-computer-science.html

digital nova scotia