ROCHESTON® CERTIFIED CYBERSECURITY SPECIALIST

Certified by Rocheston®

RCCS® Certification Program Guide

Introducing Cybersecurity

Cyberthreats are real! In the explosive volatile cyberspace of the contemporary world, threats and crimes are no longer confined in the physical domain, but have crossed over into the virtual one. The **Securityone®** is a next generation program offering the student a comprehensive understanding of fundamental cybersecurity approaches that need to be addressed within the ever-changing cyberspace.

Why Cybersecurity is a Challenge?

Cybersecurity has become a challenge, even for tech geniuses, and of course, for those who may not be technically inclined. It is difficult for many to assess risks, apply certain tools and enforce solutions. Most of the time, we have to depend on experts to tell us what to do. In an increasingly volatile virtual space, the challenges need to be appreciated by all of us, to keep our data and ourselves protected. With Securityone® training, you will be able to take better control of your own privacy, and also help others overcome cyber challenges.

Why Cybersecurity Training is Essential for "the Rest of Us"

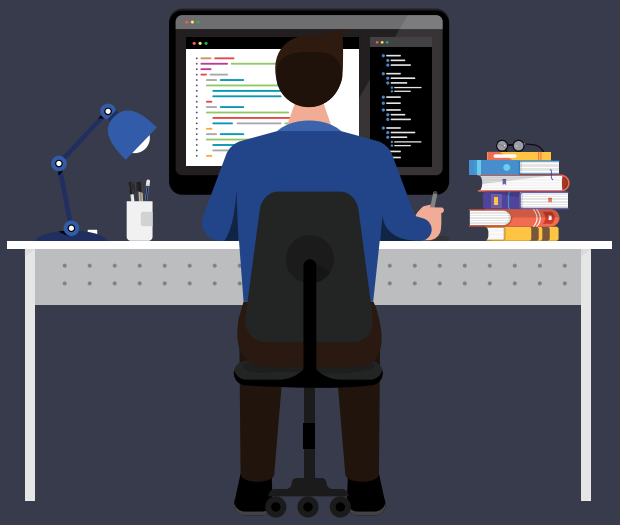
Cybersecurity is no longer just for **cybersecurity professionals. Securityone®** cybersecurity education is tailor-made for the rest of us, i.e. everybody.

All of us use digital devices, so it follows that we should be trained in cybersecurity. All students and organizational employees should be educated in cyber situational awareness looking at the latest developments in vulnerabilities, viruses and malware, threat intelligence, security alerts etc. A basic understanding will help them avoid potential threats and possible breaches in security.

What will you learn from Securityone®
Cybersecurity Training?

Learn to identify the challenges

First and foremost, of course, know the challenges in the cyber environment. Since every individual today, whether a school student or an office employee, or even a homemaker, is knee-deep in digitization, it is vital that all of us should at least possess basic awareness and knowledge to keep our systems and ourselves safe.



Learn how to safeguard a company's/individual's privacy

Being aware of the potential threats and knowing how to address them will add a layer of protection to the company's as well as the individual's data.

Learn to save time, energy and money

Every attack on an organization's digital identity costs them valuable time and effort to respond to the breaches and of course, leads to heavy financial losses. Training in cybersecurity will help the organization keep their money, and be more productive.

Learn to be less anxious

Institutions and companies can be less anxious about confidential data being breached, thus keeping customers happy and the company safe.

Become an expert yourself

The user no longer has to rely solely on technical expertise, but can enforce basic security controls without having to wait for support. The course will help regular people handle their digital footprint securely.

Who needs Securityone® Training?

Securityone® is for everybody! Any individual, organization, government agency, including schools and colleges, would benefit from the course. **Most importantly, the course is designed for ordinary day to day users who do not have the advantage of specialized technical knowledge**, i.e. for the rest of us.

The Securityone® will primarily provide you with a working knowledge of all the fundamental threats to cybersecurity in our everyday life, and how to deal with them. Every end user, that is almost every single one of us in today's world, **who has a minimum digital footprint, is in need of being educated in the ways to secure their devices and systems.** Join us in our endeavors to enable a cyber secure life for everyone.

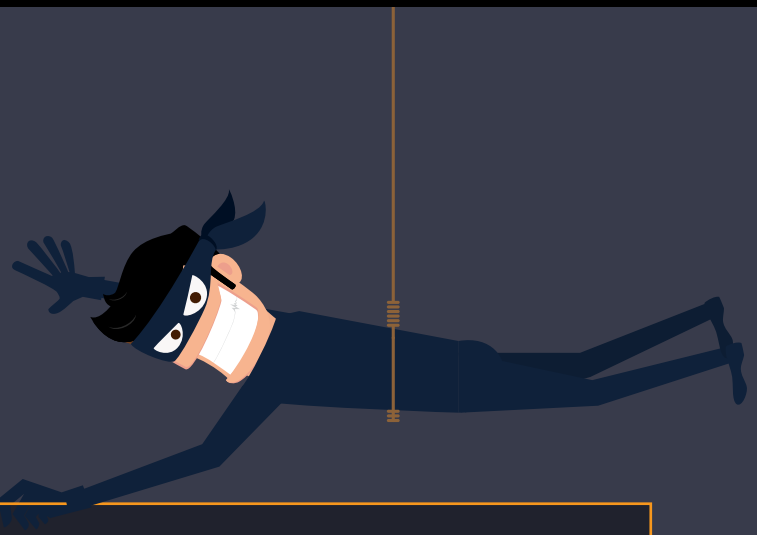
Why Securityone ® ?

The Securityone® course will provide you with **credible recognition as a Cybersecurity Specialist**. Best practices in next generation cybersecurity would make the Cybersecurity Specialist the most coveted officer in all major enterprises in the next few years.

Not only that, the course would be ideal even for non-technical people, and for day to day activities ranging from that of school students and housewives, to front end users at offices and overall everyday users of digital technology who need to have their data protected.

Securityone® enables you to gain better **control over your own devices and data, and puts you in a better position** to face the challenges to cybersecurity.

Top 15 Cyber Threats faced by Office Users



- Hacking
- Spam
- Phishing Attack
- Malware
- Ransomware
- Botnet
- Data Corruption and Data Leak
- Spoofing
- Sniffing
- DoS
- Trojans
- Rootkits
- Password Attack
- Advanced Persistent Threats
- Human Error

Hacking

Remember those hooded guys in dark rooms spending hours hunched over a computer? Well, most of them are hackers. Hacking refers to the process by which unauthorized access is gained into a digital device. Hackers are often technical geniuses, however not all of them have criminal intent!

Spam

All of us who have email accounts are aware of this particular nuisance. Spam is unwanted

Phishing Attack

Unsolicited emails, especially those asking for personal information, financial details, spelling mistakes, unwanted attachments are some ways by which cyber criminals endeavor to phish users. Phishing refers to how the attacker ‘fishes’ for information from the user using various kinds of bait.

Malware

Malware is any malicious software that once it gains access into your system, can wreak havoc. Malware generally refers to any botnet, virus, worm, spyware and Trojans, rootkits that could get into the system and corrupt it from within.

Ransomware

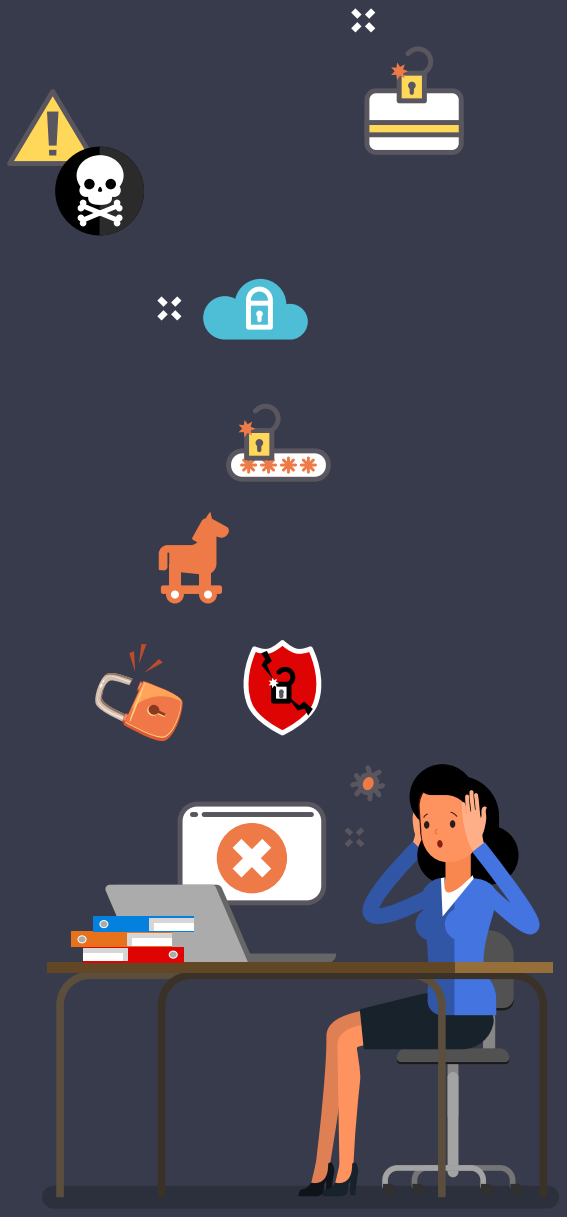
Ransomware is similar to malware i.e. it damages a system by gaining unauthorized access to it. However, in case of a ransomware, the hacker who masterminds it usually holds it over the particular person or agency whose network has been infected.

Botnet

Botnet stands for robot and network merged together. It basically refers to a multiplicity of networks that an attacker brings under his own control. Botnets are hacking tools used by the cyber criminals to remotely control other computers.

Data Corruption and Data Leak

This happens when data is rendered unreadable and becomes corrupted. Confidential data leak could cost a company billions, as well as customers and reputation.



Spoofing

Spoofing refers to a malicious practice whereby communication is sent in the guise of a source that would be familiar to the receiver. It is the practice of forging an address, making an email id look like it has been sent from a trusted source.

Sniffing

Secretly eavesdropping on existing traffic is referred to as sniffing. Sniffing data can lead to loss of private information. Passwords, private data, email traffic can all be sniffed.

DoS

Denial-of-service (DoS) is any type of cyber attack where the attackers endeavor to halt activities in a system by preventing users from accessing the service.

Trojans

These are malicious code that are given the appearance of benign applications but are here to steal, destroy your computer from within.

Rootkits

Rootkits are associated with other forms of malware such as viruses and worms. It enables the controller of the rootkit to remotely implement certain functions within the system without the owner's knowledge.

Password Attack

Attacking a system by cracking open its password or simply accessing it in an unauthorized manner is known as password attack. An office under such a siege could lead to major consequences in its network, if its login credentials are leaked.

Advanced Persistent Threats

These are continuous stealth operations carried out by hackers to gain access into a target system and could go undetected for long periods of time.

Human Error

This is one of the main factors leading to crucial crisis in the office's network and online presence. Irresponsible use of digital devices could expose an entire office to cyber threats.

A cybersecurity education program will teach you to minimize the risk of breach incidents

- Identify the threats in your environment that could be detrimental to cybersecurity
- Note if the threat is coming from users and human error
- Try to identify how, if at all, users are creating IT risks
- What are the potential vulnerabilities in your system and how can they be targeted, due to user misuse
- Note the gaps in the network
- Find ways to improve security infrastructure
- Educate your employees on the importance of cyber security

Top 10 Cyber Threats faced by Students

- Cyber predators
- Cyberbullying
- Anonymous Sharing
- Direct Messaging
- Email Attachments
- Media Streaming Sites
- Online Video Games
- Old Posts
- Identity Theft
- Illegal Content

Cyber Predators

Cyber predators scour the internet to lure innocent kids and abusing their trust and eventually luring them into revealing sensitive media or information. Children/ students should communicate to whom they are talking to on social media or on chat rooms.

Cyberbullying

This is one of the biggest cyber threats facing your young one, whether it is a young child or a young adult. Protecting yourself and your child from cyber bullying, cyber stalking, online harassment and exploitation is one of the most massive challenges in the current digital scenario. Fraud prevention and prevention of victimization are major challenges that need to be addressed every day.

Anonymous Sharing

Anonymous sharing seen in apps like Snapchat allows temporary sharing of pictures of videos. Cyber bullies or hackers can screenshot information or personal images before they disappear. Though anonymous sharing is healthy, they shouldn't overshare sensitive information.

Direct Messaging

While social media apps offer a variety of messaging services, it is also a popular place for cyber thieves who claim that the users' account is hacked, to share suspicious links or to ask for personal information.

Email Attachments

Phishing emails are powerful way to scam students and children that can be personalized to match their interests. A mismatched or bad link from an unknown source can end up infecting or injecting a malware into a personal PC.

Media Streaming Sites

Video streaming sites li ke YouTube which streams about a billion hours per day is an attractive platform for cyber criminals. The description section and the comment section are used to post links that can end up infecting the users' devices with malware.

Online Video Games

Most games hosted online are free and rely on pop-up ads to generate revenue. They also have built-in chat apps, where users might be prompted for the username and password or inappropriate content thought chat.

Old Posts

Anything posted on the internet is not temporary. Teenagers do not think about how a post might be offensive to a future boss or prospective spouse or even fall in the wrong hands of cyber bullies. Awareness should be created on what type of posts that can be posted on the internet

Identity Theft

While social media sites encourage users to share their information, most students/teens fill out complete information including birth date and name, making them vulnerable to identity theft.

Illegal Content

Torrents can offer a range of free content that can be downloaded with the help of an app. Besides the ethical perspective of downloading illegal content, the downloaded content can also conceal malware within certain files. Students should be aware of legitimate sites to download free music, videos or images.

Who needs Securityone® training?

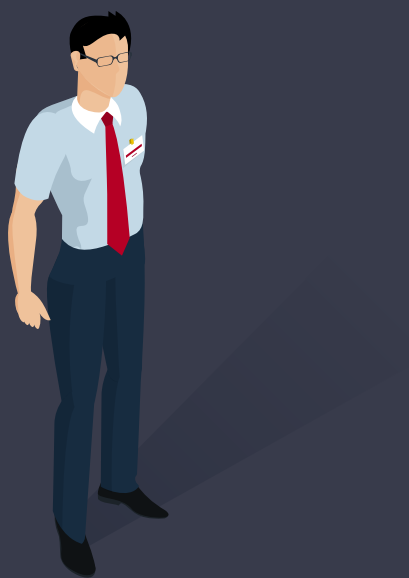
Everybody! Any individual, organization, government agency, including schools and colleges, would benefit from the course. Most importantly, the course is designed for ordinary day to-day users who do not have the advantage of specialized technical knowledge, i.e. for the rest of us.

The Securityone® will primarily provide you with a working knowledge of all the fundamental threats to cybersecurity in our everyday life, and how to deal with them. Every end user, that is almost every single one of us in today's world, who has a minimum digital footprint, is in need of being educated in the ways to secure their devices and systems. Join us in our endeavors to enable a cyber secure life for everyone.

A cyber-skills shortage means students are being recruited to fight off hackers

There aren't enough cybersecurity workers out there—and things are getting worse. According to one estimate, by **2021 an estimated 3.5 million cybersecurity jobs will be unfilled**. And of the candidates who apply, fewer than one in four are even qualified.

Universities have been training college and school students alike, to fight against hackers, which makes total sense. At Rocheston, that's exactly what we do. Train schools students to fight hackers using ou

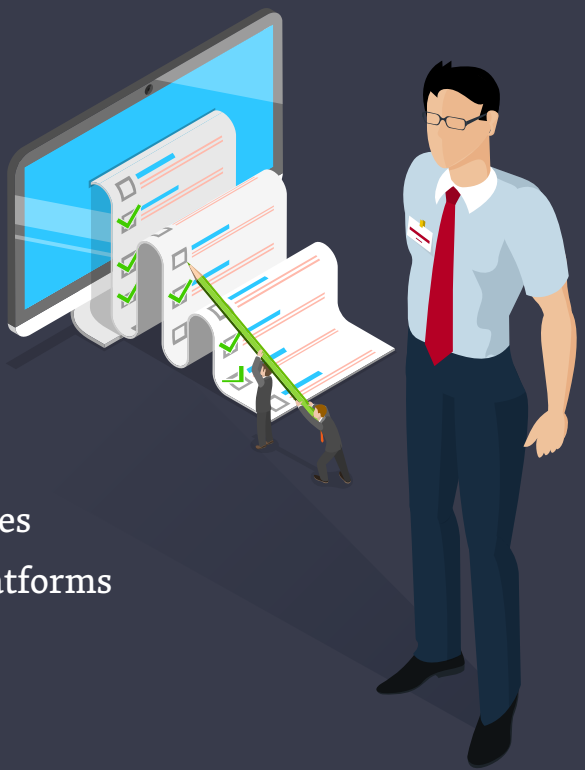


What are the Roles/Responsibilities of a Rocheston Certified Cybersecurity Specialist (RCCS)?

A few years from now, the Cybersecurity Specialist will have one of the most vital roles to perform within an organization, or even to secure an individual user's system.

Some of his responsibilities include the following:

- Assess security strategies for your networks
- Put up defensive systems against unauthorized access
- Configure security tools such as firewalls, anti-virus software etc
- Define access privileges, vulnerabilities
- Identify loopholes and enforce risk management
- Conduct audits and routine security check
- Develop incidence response solutions in the event of a breach
- Educate colleagues in security protocols and procedures
- Recommend security updates and create sustained platforms for cybersecurity



How do I join SecurityOne® Training?

The course is conducted via our Cyberclass® e-learning platform.

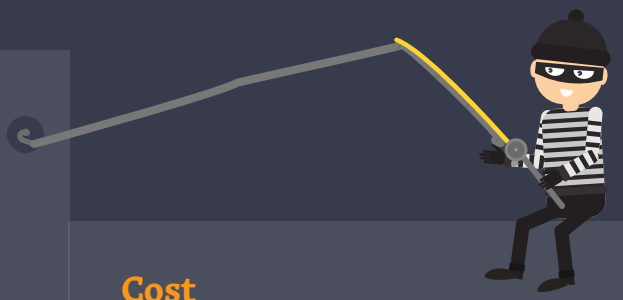
SecurityOne® training consists of:

- Courseware
- Training slides
- Videos
- Whitepapers
- Cybersecurity best practices
- Cybersecurity assessment and tools
- Lab exercises
- Self-assessment tests

Rocheston Certified Cybersecurity Specialist (RCCS) Exam

What the course will consist of:

- A 5-day Training Program
- Time: 9:30 AM – 6 PM
- The Provision of an Active Web Portal
- Seminars Conducted by Qualified Engineers
- Best in-class environment
- Exam can be taken on Rocheston Cyberclass or Pearson VUE testing platform.



Cost

For pricing in your region, please contact the local distributor.

RCCS Certificate

ROCHESTON® CERTIFIED
CYBERSECURITY SPECIALIST

THIS CERTIFICATE IS PRESENTED TO

Jason Springfield

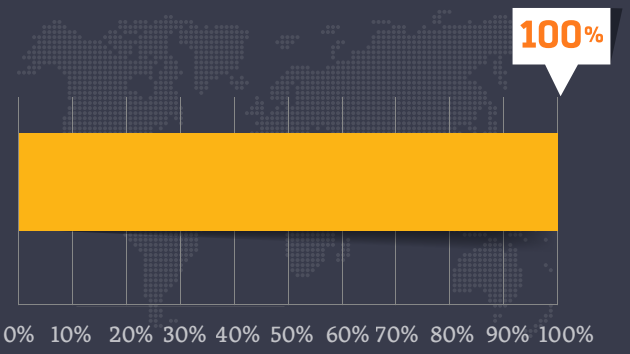
FOR COMPLETING ALL THE REQUIREMENTS TO BECOME A
ROCHESTON CERTIFIED CYBERSECURITY SPECIALIST

HAJA MOHIDEEN
PRESIDENT & CEO

rccs

Cybersecurity Jobs - The Way Forward

Artificial Intelligence Will Change 100 Percent of Jobs. Technology is going to change everyone's job. It means reskilling of your current skills that apply for the future, says IBM CEO.

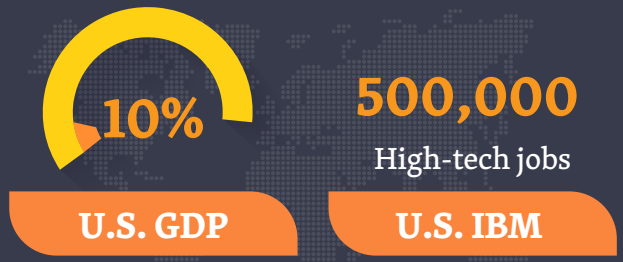


Companies that don't incorporate AI today will soon become outdated tomorrow. Similarly, if you don't update your professional skills today, then your job will be replaced by AI robots tomorrow.

According to the World Economic Forum, the value of digital transformations in the Fourth Industrial Revolution is estimated at in the next 10 years alone, across all sectors, industries, and geographies.

The technology sector accounts for 10 percent of U.S. GDP and is the fastest part of the American economy but there are not enough skilled workers to fill the 500,000 open high-tech jobs in the U.S. IBM says: 77% of Enterprises Don't Have a Cybersecurity Incident Response Plan. Cyberattack on these organizations is inevitable.

They don't have a cybersecurity incident response plan applied across the enterprise, according to a study conducted by IBM. One of the primary reasons for this is the cybersecurity engineers shortage. It's a major, major problem for the cybersecurity industry.



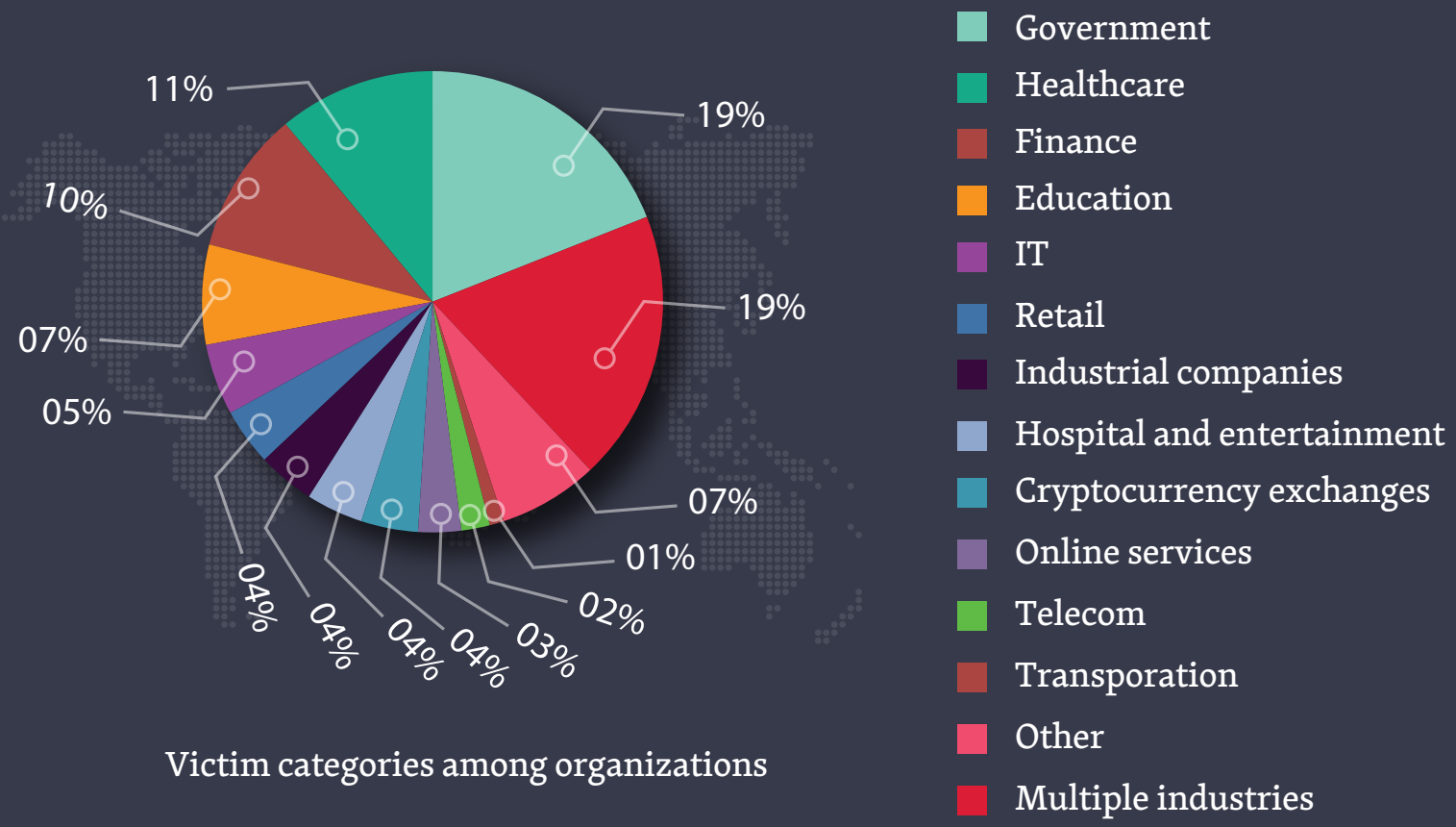
Enterprises Don't Have a Cybersecurity

Latest Trends and Statistics in Cyberthreatscape

In the parlance of the dark web, attackers these days want to 'own' your entire system."

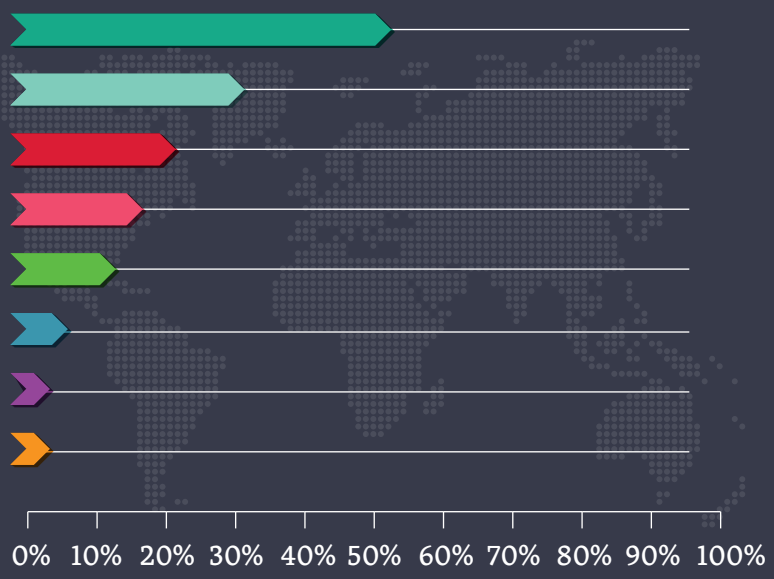
Tom Kellermann,
Carbon Black's Chief Cybersecurity Officer.

- According to Carbon Black, about 50% of all cyber attacks these days leverage “island hopping.” whereby some networks are leveraged to reach other connected networks.
- 56% incident response partners have faced attempted counter-incidents in the first quarter of 2019.
- The financial and healthcare sectors are some of the most targeted industries for these attacks.
- From the third quarter of 2018, about 70% of all respondents surveyed witnessed cyber attacks on the finance sector.
- About 61% respondents encountered the same in healthcare.
  59% fell victim in manufacturing.



Victim categories among organizations

- **In 2018, 51% of cases had theft of confidential data** as a primary. objective. State-run websites are targeted to grab public attention.
- Hacktivist **attacks accounted for nearly 1/4th of all events**. The data of 6 million people was compromised in 2018, consisting of personal data and healthcare related information.
- Ransomware was a common occurrence in healthcare, as persistent operations are key. **Hancock Regional Hospital in the U.S.A. paid 55k US$** in ransom to obtain control over their own systems. **65% of events against financial institutions were profit-driven.**
- In educational institutions, the damages amounted to around 2 million US$ in 2018. 1/6th of attacks were ransomware related.
- E-commerce stores and portals were targeted, with **70% of attacks aimed at data theft**. (customer information) 5 million cards were compromised.
- VPN filter **malware compromised >500,000 routers**. In another incident, hackers stole **private data from 383,000 guests who were at the Marriott Hotel chain**. The entity's stocks fell by 6% in a single day.
- At the individual level, social engineering accounted for 43% of incidents.
- **Malware made up 73%** of incidents.
- **Spyware infection accounted for 21%** of incidents.
- Mining witnessed a decrease in popularity and it's share among malware attacks against **individuals decreased from 27% to 13%.**
- 2018 was marked by the two biggest **DDoS attacks in history, reaching 1.35 and 1.7 terabits per second.**



56% Malware use
31% Social engineering
21% Hacking
17% Web attacks
14% Credential compromise
03% DDos
01% Abuse of legitimate software
01% other

ROCHESTON® CERTIFIED CYBERSECURITY SPECIALIST

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

ROCHESTON® CERTIFIED CYBERSECURITY SPECIALIST

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

ROCHESTON® CERTIFIED CYBERSECURITY SPECIALIST

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

ROCHESTON®

BE EXCEPTIONAL