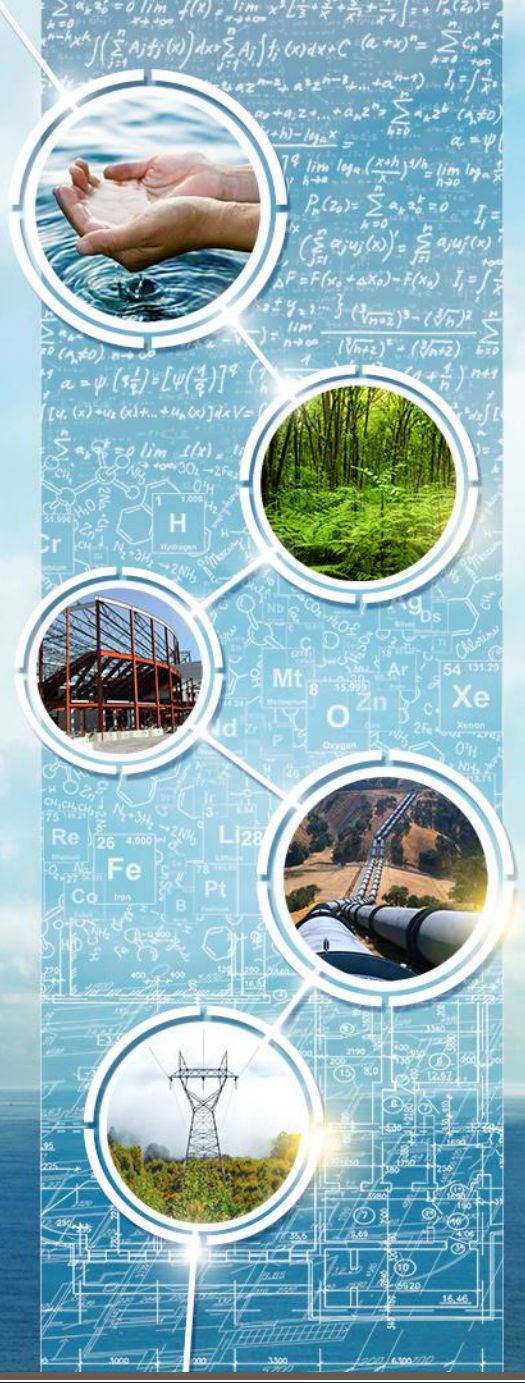


IP3
A Tetra Tech Company

Cybercrime and Cyber Security

September 16, 2019

Judith Hellerstein
CEO
Hellerstein & Associates
& Kelly Wong
Professor
University of Maryland

Agenda

Agenda

- Definitions of Cybercrime and Cyber Security
- Examples of Cybercrimes
- Cybercrime Laws
- Domestic and International Agencies responsible for Cybercrime and cyber security
- Tools available to prevent Cybercrime
- Best Practices

CyberCrime Definition

- Cybercrime is any criminal activity that involves a computer, networked device or a network.
  - While most cybercrimes are carried out to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials.
  - Some cybercrimes do both -- i.e., target computers to infect them with viruses, which are then spread to other machines and, sometimes, entire networks.
- Cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud and identity fraud, as well as attempts to steal financial account, credit card or other payment card information.
- Cybercriminals may target private personal information, as well as corporate data for theft and resale.

Cyber Crime Definition

- The U.S. Department of Justice divides cybercrime into three categories:
  - crimes in which the computing device is the target, for example, to gain network access;
  - crimes in which the computer is used as a weapon, for example, to launch a denial-of-service (DoS) attack; and
  - crimes in which the computer is used as an accessory to a crime, for example, using a computer to store illegally obtained data.
- The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, defines cybercrime as a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements.
  - Other forms of cybercrime include illegal gambling, the sale of illegal items, like weapons, drugs or counterfeit goods, as well as the solicitation, production, possession or distribution of child pornography.

International Definition

- There is no international definition of cybercrime nor of cyberattacks.
- Crimes typically cluster around the following categories:
  - i) Crimes against the confidentiality, integrity and availability of computer data and systems;
  - ii) computer-related crimes;
  - iii) content-related crimes;
  - iv) crimes related to infringements of copyright and related rights.
- According to the UN, Cybercrime requires an ICT infrastructure. It is often typified as the creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure (e.g. the cyber-takeover of a power-plant by an organized crime group) and taking a website offline by overloading it with data (a DDOS attack).

Definition (Continued)

- Cyber crime is any action which can occur in the offline world but can also be facilitated by ICT. This typically includes online frauds, purchases of drugs online and online money laundering.
- Child Sexual Exploitation and Abuse includes abuse on the clear internet, darknet forums and, increasingly, the exploitation of self-created imagery via extortion - known as "sextortion".
- The online publication of racist and xenophobic propaganda via computer networks is now a criminal act and also Cybercrime.

Cybercrime Activities

- Cybercriminal activity may be carried out by individuals or small groups with relatively little technical skill or by highly organized global criminal groups that may include skilled developers and others with relevant expertise.
  - cybercriminals often choose to operate in countries with weak or nonexistent cybercrime laws.
- Cybercriminals often carry out their activities using malware and other types of software, but social engineering is often an important component for executing most types of cybercrime.
- Phishing email is an important component to many types of cybercrime, but especially so for targeted attacks, like business email compromise where the attacker attempts to impersonate, via email, a business owner to convince employees to pay out bogus invoices.

Cyber Crime and Internet Privacy

- Internet privacy is cause for concern for any user planning to make an online purchase, visit a social networking site, participate in online games or attend forums.
  - If a password is compromised and revealed, a victim's identity may be fraudulently used or stolen.
- Typical Cyber Crimes include:
  - Phishing: An Internet hacking activity used to steal secure user data, including username, password, bank account number, security PIN or credit card number.
  - Pharming: An Internet hacking activity used to redirect a legitimate website visitor to a different IP address.
  - Spyware: An offline application that obtains data without a user's consent. When the computer is online, previously acquired data is sent to the spyware source.
  - Malware: An application used to illegally damage online and offline computer users through Trojans, viruses and spyware.

Types of CyberCrime

- There are many different types of cybercrime; most cybercrimes are carried out with the expectation of financial gain by the attackers.
  - Cyberextortion, is crime involving an attack or threat of attack coupled with a demand for money to stop the attack, for example--Ransomware
  - Ransomwear--a form of cyberextortion in which the victim device is infected with malware that prevents the owner from using the device or the data stored on it. To regain access to the device or data, the victim has to pay the hacker a ransom.
  - Cryptojacking, uses scripts to mine cryptocurrencies within browsers without the user's consent
  - Identify theft, occurs when an attacker accesses a computer to glean a user's personal information that they can then use to steal that person's identity or access bank or other accounts.
  - Credit card fraud, occurs when hackers infiltrate retailers' systems to get the credit card and/or banking information of their customers. Stolen payment cards can be bought and sold in bulk on darknet
  - Cyberespionage--occurs when a cybercriminal hacks into systems or networks to gain access to confidential information held by a government or other organization

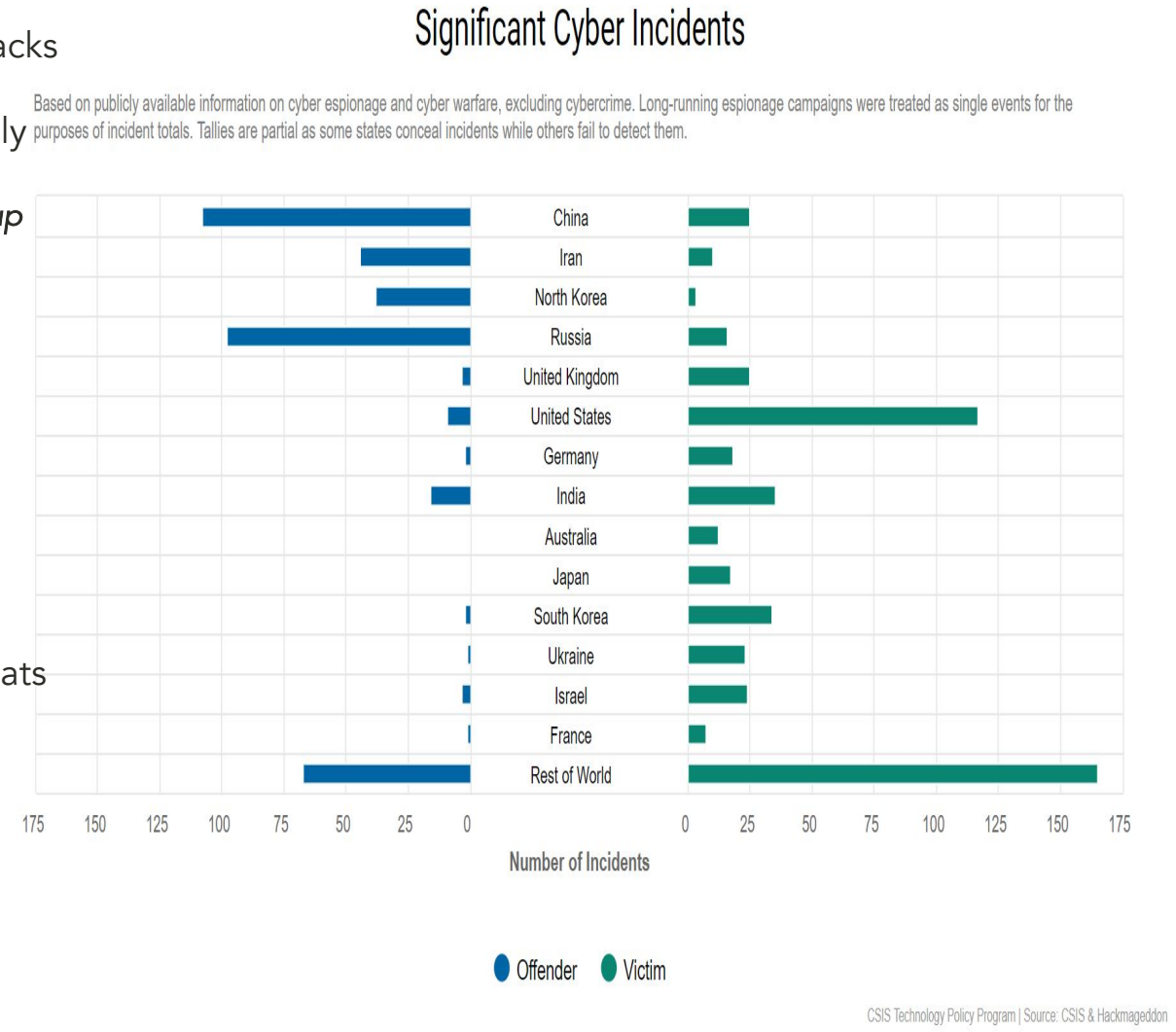
Ransomware

- Ransomware attacks are not only proliferating, they're becoming more sophisticated.
- In the past, ransomware was normally delivered through spam e-mails, but because e-mail systems got better at filtering out spam, cyber criminals turned to spear phishing--e-mails targeting specific individuals, or are seeding legitimate websites with malicious code, taking advantage of unpatched software on end-user computers.
- In the last few months several US cities were victims to Ransomware attacks
  - These include: Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—these are just some of the entities impacted by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them.

Common Adversaries

- Cybercrime types
  - Most prolific are nation state attacks for IP theft/espionage
  - Disruption of networks and supply chains
    - *WannaCry and NotPetya - wakeup call for all 3 countries, et .al, approx.($15B internationally)*
  - Critical infrastructure top targets
    - Public/government
    - Telecommunications
    - Health
    - Academic
    - Manufacturing
    - Power/utility, and
    - transportation
  - General information warfare threats

- Costs from theft, threat analysis, mitigation, and recovery
  - Globally = 1% of GDP in 2018
  - From 2017 -2018
    - Japan (+31%)
    - UK (+30%)
    - US(+29%)



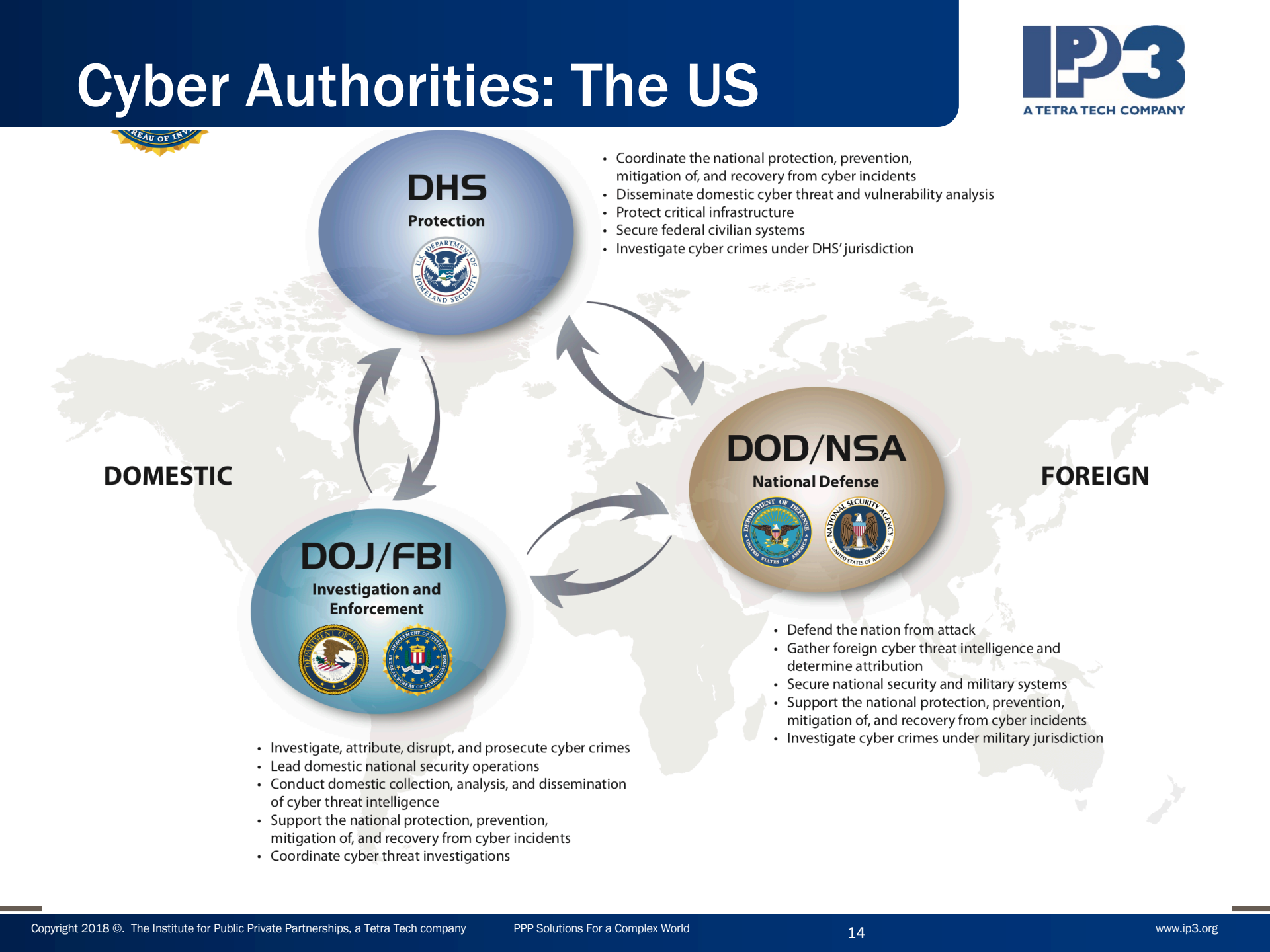
Source: Accenture 2019 Global Cost of Crime Study

- Cyberspace accountability for nations can include developing comparable security, resiliency, and attribution.
  - These capabilities are critical for national security.
- While cyber security is foundational to protect assets from an attack happening in the first place. Cyber resiliency concerns the assurances for a nation that its critical infrastructures will remain effective and operational for it to endure inevitable attacks.
- Attribution of responsible attackers is a capability enabled by threat intelligence analysis of multiple sources of information to learn tactics, techniques, and procedures used by attackers. This information enhances methods for security and resiliency.
- Transparency of these capabilities, propensity for risk, and cultures are challenges to national cyber strategies being comparable to protect our tightly woven digital economies.

Cybercrime (Continued)

- Cybercrimes may have public health and national security implications, making computer crime one of the Department of Justice's top priorities.
- In the US, Cybercrime is split between the FBI and the Computer Crime and Intellectual Property Section (CCIPS) within the US Department of Justice.
- The FBI is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists.
  - Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated.
  - Cyber criminals target a country, State, or City critical infrastructure, including both private and public sector networks.
  - Companies are targeted for trade secrets and other sensitive corporate data and universities for their cutting-edge research and development.
  - Citizens are targeted by fraudsters and identity thieves, and children are targeted by online predators

Cyber Authorities: The US



- Coordinate the national protection, prevention, mitigation of, and recovery from cyber incidents
- Disseminate domestic cyber threat and vulnerability analysis
- Protect critical infrastructure
- Secure federal civilian systems
- Investigate cyber crimes under DHS' jurisdiction

- Investigate, attribute, disrupt, and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate cyber threat investigations

- Defend the nation from attack
- Gather foreign cyber threat intelligence and determine attribution
- Secure national security and military systems
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Investigate cyber crimes under military jurisdiction

CCIPS

- US DOJ's CCIPS office works with local, state, and International Governments to provide capacity building and technical assistance on Cybercrimes.
  - CCIPS is responsible for implementing national strategies to combat computer and intellectual property crimes worldwide.
  - CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts.
  - Section attorneys work to improve the domestic and international infrastructure-legal, technological, and operational-to pursue network criminals most effectively.

Electronic Crimes Task Force

- The Secret Service's Electronic Crimes Task Force (ECTF) investigates cases that involve electronic crimes, particularly attacks on the nation's financial and critical infrastructures.
  - The Secret Service also runs the National Computer Forensics Institute (NCFI), which provides state and local law enforcement, judges and prosecutors with training in computer forensics.
  - The Internet Crime Complaint Center (IC3), a partnership between the FBI, the National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance (BJA).
  - This group accepts online complaints from victims of internet crimes or interested third parties.

NIST/Homeland Security

- The US's National Institute of Standards and Technology (NIST) issued guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model.
  - Companies must be prepared to "respond to the inevitable cyber incident, restore normal operations, and ensure that company assets and the company's reputation are protected.
- In the US, the Department of Homeland Security (DHS) is the agency responsible for Cybersecurity and for strengthening the security and resilience of cyberspace
- The international community has been trying to develop cybernorms for international behavior for over a decade.
  - This has been happening through UN processes, through the UNODC, the Global Commission on Cyberspace (GCCS), through international law discourse, and other fora.

Cybercrime Law

- The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty seeking to address Internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.
  - It was drawn up by the Council of Europe in Strasbourg, France, with the active participation of the Council of Europe's observer states Canada, Japan, Philippines, South Africa and the United States.
  - The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001 and was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004.
  - As of March 2019, 63 states have ratified the convention, while a further four states had signed the convention but not ratified it.

Budapest Convention

- The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security.
  - It contains a series of powers and procedures such as the search of computer networks and lawful interception.
  - Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.
    - Harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime
    - Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form
    - Setting up a fast and effective regime of international cooperation

Budapest Convention (continued)

- It also sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data.
- Additionally, the Convention contains a provision on a specific type of transborder access to stored computer data and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Signatory Parties
  - This means that if a crime happens in the US, the US focal point can call up a focal point in another country and ask them to freeze and collect certain electronic data to avoid its destruction without having to go through the courts system or a mutual assistance process

International Organizations

- Within the UN, the UN Office of Drugs and Crime (UNODC) has leadership over Cybercrimes and not the ITU.
- UNODC was given responsibility over Cybercrime by the UN, specifically General Assembly resolution 65/230 and Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8.
- UNODC is a global leader in the fight against drugs and international crime.
  - Established in 1997 through a merger between the United Nations Drug Control Program and the Centre for International Crime Prevention, UNODC operates in all regions of the world through an extensive network of field offices.
- UNODC provides capacity building to all UN Member States.
  - Training manuals and the adoption of codes of conduct and standards and norms are some examples of this capacity building that aim to guarantee that the accused, the guilty and the victims can all rely on a criminal justice system that is fair and grounded on human rights values.

UNODC

- Prior to the these resolutions and the start up of UNODC's Global Program, UNODC's open-ended intergovernmental expert group conducted a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector.
  - This work included the exchange of information on national legislation, best practice, technical assistance and international cooperation. This are all listed in the Cybercrime Repository available to all.
- The Global Program on Cybercrime is mandated to assist Member States in their struggle against cyber-related crimes through capacity building and technical assistance.
- UNODC provides technical assistance in capacity building, prevention and awareness raising, international cooperation, and data collection, research and analysis on cybercrime.

Cybercrime Repository

- The Darknet is a collection of thousands of websites that use anonymity tools like TOR to encrypt their traffic and hide their IP addresses.
  - The high level of anonymity in the digital space enables criminals to act without being easily detected.
  - The darknet is most known for black-market weapon sales, drug sales and child abuse streaming.
- UNODC's cybercrime repository is a central data repository of cybercrime laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance.
- It was developed as a central data repository of cybercrime laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance (Resolution 22/8 of the Commission of Crime Prevention and Criminal Justice, entitled 'Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime').
  - The repository consists of three databases: Case Law, Cybercrime Legislation, Lessons Learned. There is also a space for Contributor contributions, which are reviewed and verified before adding to the other 3 databases.

Cybercrime Repository

- The Case Law Database contains jurisprudence, as well as records of successful law enforcement operations, on cybercrime and crimes related to electronic evidence.
  - This allows users to see how Member States are tackling cybercrime cases both operationally and in their courts.
- The Legislation Database contains cybercrime and procedural laws and is searchable by country, cybercrime offence, and procedural aspects.
  - the Database provides extracts of laws relevant to specific cybercrime offences and cross-cutting issues, allowing the user to quickly find provisions relating to the search query.
- The Lessons Learned database contains national practices and strategies in preventing and combating cybercrime.
  - Information compiled in this database has been gathered in the framework of the UNODC Comprehensive Study on Cybercrime (2013) and is supplemented by national cybercrime and cybersecurity strategies.

The GCSC

- Another International institution is the Global Commission on the Stability of Cyberspace (GCSC) (a multistakeholder commission of experts).
- The GCSC is charged with developing proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace
  - One of the outcomes of the 2015 GCCS meeting in The Hague was the establishment of 'the Global Forum on Cyber Expertise'.
  - Their declaration not only sets out an agenda around five themes (Cyber Security Policy and Strategy, Cyber Incident Management and critical Infrastructure Protection, Cybercrime, Cyber Security Culture and Skill, and Cyber Security Standards), it also clearly defines its guiding principles for reaching these goals.

Global Forum on Cyber Expertise

- The Global Forum on Cyber Expertise (GFCE) is a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building.
  - It was founded in 2015 and came out as an outgrowth of the Global Conference on Cyber Space (GCCS) that took place in The Hague, The Netherlands in that year
  - The aim is to identify successful policies, practices and ideas and multiply these on a global level.
  - It works with almost 80 partners from NGOs, the tech community and academia GFCE members to develop practical initiatives to build cyber capacity.
  - The Members (79) and Partners (19) cooperate on projects called initiatives. These initiatives are focused on different topics, such as awareness raising, CIIP, cybercrime training, and internet infrastructure, either with a global or with a regional focus.

GFCE Focus

- In 2017, the GFCE's focus shifted from building and expanding the network to positioning the GFCE as a coordinating platform for Cyber Capacity Building.
- In November 24th 2017, the GFCE community endorsed the Delhi Communiqué which prioritized five themes in Cyber Capacity Building and calls for action to jointly strengthen global cyber capacities. The five identified themes are:
  - Cyber Security Policy and Strategy;
  - Cyber Incident Management and Critical Information Protection;
  - Cybercrime;
  - Cyber Security Culture and Skills;
  - Cyber Security Standards.
- Five working groups were created to focus on one of these five themes to strengthen international cooperation by developing a common focus, enabling efficient use of the available resources and avoiding duplication of efforts.
- In 2019, the aim will be to facilitate and to coordinate knowledge and expertise sharing for the implementation of Cyber Capacity Building.

GFCE Best Practices

- GFCE has published best practices on the following topics
  - National Cyber Security Assessments
  - National Computer Security Incident Response
  - Incident capture and analytics
  - Critical Information Infrastructure Protection
  - Legal Frameworks
  - Law enforcement in cyberspace
  - Cyber Security Awareness
  - Standards

Global Cyber Alliance

- The Global Cyber Alliance (GCA) is an international, cross-sector effort dedicated to eradicating cyber risk and improving our connected world. They achieve their mission by:
  - Uniting Global Communities
  - Implementing Concrete Solutions that reduce and eradicate cyber risk and make tools freely available to all
  - Measuring effectiveness.
- It was founded in September 2015 by the Cities of NYC and London along with the Center of Internet Security to address systemic cyber risk through a proactive risk-based, solution oriented approach to address and eradicate malicious cyber risks.
- Its goals is to help other organizations, Governments, and businesses, (large and small) prevent cyber crimes and enhance their cyber security by sharing real-time threat info across sectors.
  - Only by close collaboration between organizations and government agencies could we ensure that critical infrastructure of a city and of businesses and citizens is protected.

GCA

- Original funding for GCA came from the three main partners using money gained from criminal forfeiture laws in each of these countries.
- The GCA later expanded its partners into 17 different sectors in the economy such as
  - Aerospace
  - Civil Society
  - Communications
  - Education
  - Energy
  - Financial
  - Governments
  - Health
  - Insurance
  - Real Estate
  - Risk Management
  - Security
  - Technology
  - Telecommunications
  - Transportation
  - Travel
  - Legal
- GCA's research has found that over 80% of all cyber attacks have started from Phishing alone and led to the creation of several Toolkits and other resources.

GCA Resources

- The GCA created several toolkits to help other organizations and even local Governments better understand the risks and how to protect themselves
  - Cyber Toolkit for Small Businesses
  - Cyber Toolkit for Elections
  - Automated IoT Defense Ecosystem (AIDE)
  - DMARC--Domain-based Message Authentication, Reporting and Conformance
  - Quad 9
  - Tools to help developers using WordPress and Content Management Systems to secure their website
  - Smart Cities and IoT--This interconnectivity poses great risks, however, as cybercriminals can hack into devices and penetrate systems remotely, causing potentially catastrophic damage.

DMARC

- DMARC is the simple, trusted, free solution that brings together email authentication protocols, and adds reporting and compliance.
  - In June 2016, the U.K. government mandated that all U.K. government departments adopt DMARC, and the EU-CERT has also made a recommendation for the use of DMARC.
  - In October 2017, the U.S. Department of Homeland Security issued Binding Operational Directive 18-01, which requires the adoption of DMARC by federal civilian domains.
- Despite the tremendous benefits of DMARC, it was not being widely deployed in the public or private sectors.
  - GCA created the step-by-step DMARC Setup Guide, available in 18 languages, to help organizations of all sizes to implement DMARC.

Other GCA Resources

- Automated IoT Defense Ecosystem (AIDE) is a system that enables the automated collection, analysis, distribution, and display of attacks on IoT devices and a means to implement distributed defense of these devices including in small office or manufacturing and home environments
- Quad9 protects users from accessing known malicious websites, leveraging threat intelligence from multiple industry leaders and currently blocks up to two million threats per day for users in 76 countries.
- McScrapy evaluates a website and renders it into simple form, keeping as much functionality as possible, while removing potential vulnerabilities.
- Smart Cities and IoT—The inherent interconnectivity within IoT and the sensors used in Smart Cities poses great risks as cybercriminals can hack into devices and penetrate systems remotely, causing potentially catastrophic damage

Cyber Security Definition

- Cyber security is the practice of defending computers and servers, mobile devices, electronic systems, networks and data from malicious attacks.
  - It is also known as information technology security or electronic information security.
  - The term is broad-ranging and applies to everything from computer security to disaster recovery and end-user education.
- Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks.
- Cyber security relies on cryptographic protocols used to encrypt emails, files and other critical data.
  - This not only protects information that is transmitted but also guards against loss or theft.
  - End user security software scans computers for pieces of malicious code, quarantines this code and then removes it from the machine.

Cybersecurity (continued)

- Electronic security protocols also focus on malware detection — ideally in real time.
  - Many use what's known as "heuristic analysis" to evaluate the behavior of a program in addition to its code, helping to defend against viruses or Trojan horse's and other viruses or malware that can change their shape with each execution.
- The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves.
- Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security and then only to protect their most crucial system components and defend against known threats.
- Today, this approach is no longer sufficient, as the threats advance and change more quickly than organizations can keep up with.
  - As a result, advisory organizations need to promote more proactive and adaptive approaches to cyber security.

Effects of Ransomware

- Ransomware can be devastating to an individual or an organization.
- Anyone with important data stored on their computer or network is at risk, including government, law enforcement agencies, healthcare systems, or other critical infrastructure entities.
- Recovery can be a difficult process that may require the services of a reputable data recovery specialist, and some victims pay to recover their files.
- However, those that pay the ransom have no guarantee that they will recover their files

Ransomware attacks

- The inability to access the important data can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation.
- In the US State of Georgia in recent months, the tally of victims has been stunning: the city of Atlanta, the state's Department of Public Safety, State and local court systems, a major hospital, a county government, and a police department for a city of 30,000 people.
- Last year the city of Atlanta was attacked and the attackers demanded roughly $51,000 in Bitcoin but the City, upon advice from the FBI, refused to pay.
  - This attack cost the city over 17 million USD to rebuild its infrastructure

More Examples

- In May of 2019, the US city of Baltimore was attacked. The hackers demanded about $76,000 in Bitcoin to release the City's files and allow employees to regain access to their computers.
  - The City's Mayor declined to pay the ransom, in part because there was no guarantee the files would be unlocked. Also paying a ransom would encourage others to try
  - In the nearly four months since the attack, the city has brought systems back online one by one, spending more than $5.3 million on computers and contractors brought on to help recover from the attack.
  - An early estimate put the combination of lost revenue and city expenditures at more than $18 million.
- Some cities hit by an attack decide to pay the ransom but others refuse

How it Spreads & Consequences

- The attacks have serious consequences, with recovery costing millions of dollars.
- There is also a corresponding loss of confidence in the integrity of systems that handle basic services like water, power, emergency communications and vote counting.
- In a ransomware attack, victims—upon seeing an e-mail addressed to them—will open it and click on an attachment that appears legitimate but that actually contains the malicious ransomware code.
  - Or the e-mail might contain a legitimate-looking website address, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software.
- Once the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network.
- Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment, often in bitcoins, in exchange for a decryption key.

The Critical National Functions

- Cross cutting critical infrastructure to focus processes and identifying those that deliver critical services/functions to the nation
- Identifies in the process the systems across all vital infrastructure sectors that need to be hardened
- Identifies the series of tasks and information exchange that need to be readily secured and replicated as in disaster management and business continuity plans
- Goal = near nonstop operational effectiveness via *resiliency*

CONNECT	DISTRIBUTE	MANAGE	SUPPLY
▪ Operate Core Network ▪ Provide Cable Access Network Services ▪ Provide Internet Based Content, Information, and Communication Services ▪ Provide Internet Routing, Access, and Connection Services ▪ Provide Positioning, Navigation, and Timing Services ▪ Provide Radio Broadcast Access Network Services ▪ Provide Satellite Access Network Services ▪ Provide Wireless Access Network Services ▪ Provide Wireline Access Network Services	▪ Distribute Electricity ▪ Maintain Supply Chains ▪ Transmit Electricity ▪ Transport Cargo and Passengers by Air ▪ Transport Cargo and Passengers by Rail ▪ Transport Cargo and Passengers by Road ▪ Transport Cargo and Passengers by Vessel ▪ Transport Materials by Pipeline ▪ Transport Passengers by Mass Transit	▪ Conduct Elections ▪ Develop and Maintain Public Works and Services ▪ Educate and Train ▪ Enforce Law ▪ Maintain Access to Medical Records ▪ Manage Hazardous Materials ▪ Manage Wastewater ▪ Operate Government ▪ Perform Cyber Incident Management Capabilities ▪ Prepare for and Manage Emergencies ▪ Preserve Constitutional Rights ▪ Protect Sensitive Information ▪ Provide and Maintain Infrastructure ▪ Provide Capital Markets and Investment Activities ▪ Provide Consumer and Commercial Banking Services ▪ Provide Funding and Liquidity Services ▪ Provide Identity Management and Associated Trust Support Services ▪ Provide Insurance Services ▪ Provide Medical Care ▪ Provide Payment, Clearing, and Settlement Services ▪ Provide Public Safety	▪ Exploration and Extraction Of Fuels ▪ Fuel Refining and Processing Fuels ▪ Generate Electricity ▪ Manufacture Equipment ▪ Produce and Provide Agricultural Products and Services ▪ Produce and Provide Human and Animal Food Products and Services ▪ Produce Chemicals ▪ Provide Metals and Materials ▪ Provide Housing ▪ Provide Information Technology Products and Services ▪ Provide Materiel and Operational Support to Defense ▪ Research and Development ▪ Supply Water

National Critical Functions: The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Growth of Cyber Crime

- There is an active market for buying and selling stolen personal information, which occurs mostly in darknet markets but also in other black markets.
- People increase the value of the stolen data by aggregating it with publicly available data, and sell it again for a profit, increasing the damage that can be done to the people whose data was stolen
- A 2018 online survey from The Harris Poll reveals that nearly 60 million Americans were affected by identity theft, up from 15 million in 2017.
- Additional statistics from Norton show the US is the biggest target for cyber attacks.
- Between 2015 and 2017, 38% of the attacks occurred in the US. India ranked second with 17%, followed by Japan (11%), Taiwan (7%), the Ukraine and South Korea (both 6%), Brunei, Russia and Vietnam (each at 4%) and Pakistan (3%).

Best Practices on Cyber

- The US Department of Homeland Security which has the responsibility for Cyber Security recommends that organizations employ the following best practices:
  - Restrict users' permissions to install and run software applications, and apply the principle of "least privilege" to all systems and services.
    - Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
  - Use application whitelisting to allow only approved programs to run on a network.
  - Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
  - Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
  - Configure firewalls to block access to known malicious IP addresses.

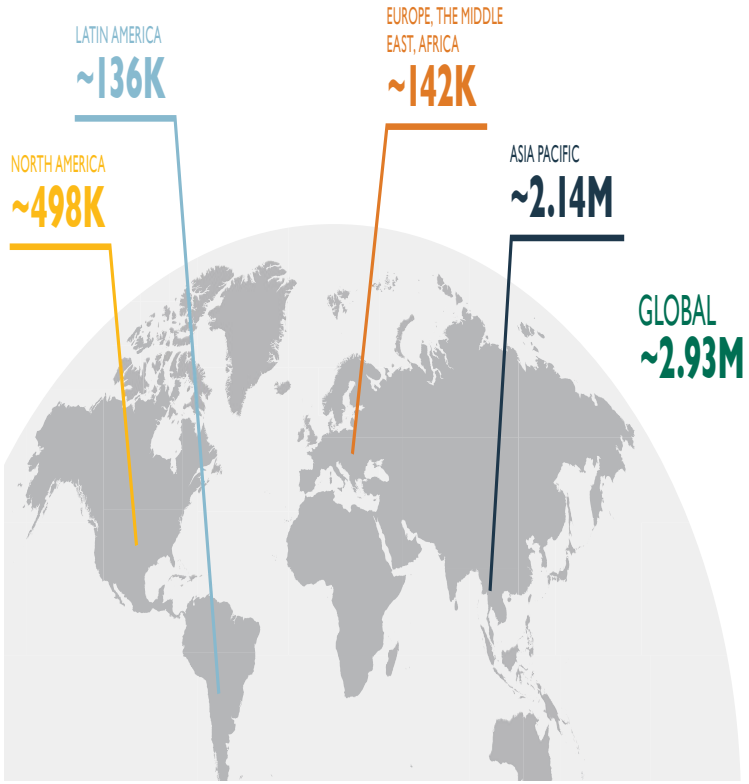
Best Practices

- Additionally, all users should follow these precautions to protect themselves against the threat of ransomware:
  - Update software and operating systems with the latest patches.
    - Outdated applications and operating systems are the target of most attacks.
  - **Never** click on links or open attachments in emails.
  - Backup data on a regular basis. Keep it on a separate device and store it offline.
  - Follow safe practices when browsing the Internet.
- In response to the attacks many cities are hardening their infrastructure and creating a cyber defense team within their offices to protect their cities

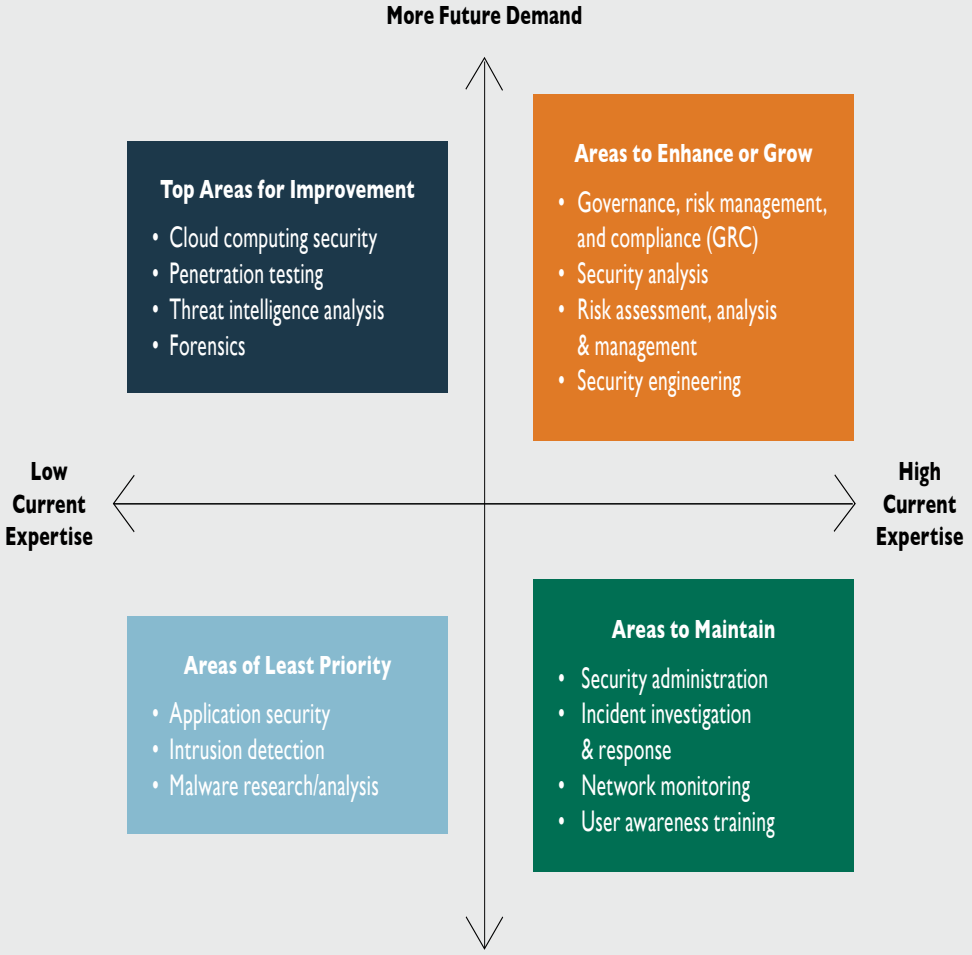
Building the Cyber Workforce

A TETRA TECH COMPANY

Gap in Cybersecurity Professionals by Region



Source: 2018 (ISC)² Cybersecurity Workforce Study



Conclusion

- Cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and Internet fraud and identity fraud, as well as attempts to steal financial account, credit card or other payment card information
- Cybercriminals may target private personal information, as well as corporate data for theft and resale
- The GCSC, the GFCE, and the GCA have been working on these issues and what types of capacity building and technical assistance they are offering
- Typical types of cyber crime: phishing, pharming, malware, ransomware
- Ransomware attacks are not only proliferating, they're becoming more sophisticated
- It is no longer safe to just protect crucial network infrastructure at the perimeter the entire organization needs protection
- There are a number of Best Practices and precautions that everyone should follow to keep their systems safe from hacking and against the threat of ransomware

Thanks

Questions, Comments, Suggestions

Judith Hellerstein

Hellerstein & Associates

Judith@jhellerstein.com

www.jhellerstein.com

What's App-+12023336517