

The State of Cybersecurity

Tracy Gregorio
CEO, G2 Ops, Inc.

Dr. Bartosz Wojszczyk
President & CEO, Decision Point Global

March 9, 2021



**INNOVATION
COLLABORATIVE
HAMPTON ROADS**

Agenda

- The State of Cybersecurity
- Threats
- Industry Feedback (Interactive)
- What's Next? (Interactive)

2019 FBI Internet Crime Complaint Center (IC3)

- The FBI's Internet Crime Complaint Center (IC3) received **467,361 complaints** in 2019 (1300 every day)
 - More than **\$3.5 billion in losses** to individuals/business victims
- One of the most financially costly complains involved **business email compromise (BEC)** with \$1.7 billion in losses and 23,775 complaints
- Other prevalent crime types reported include:
 - Phishing/Vishing/Smishing/Pharming
 - Non-payment/Non-delivery
 - Extortion
 - Personal Data Breach

Select a state: **Virginia** ↓

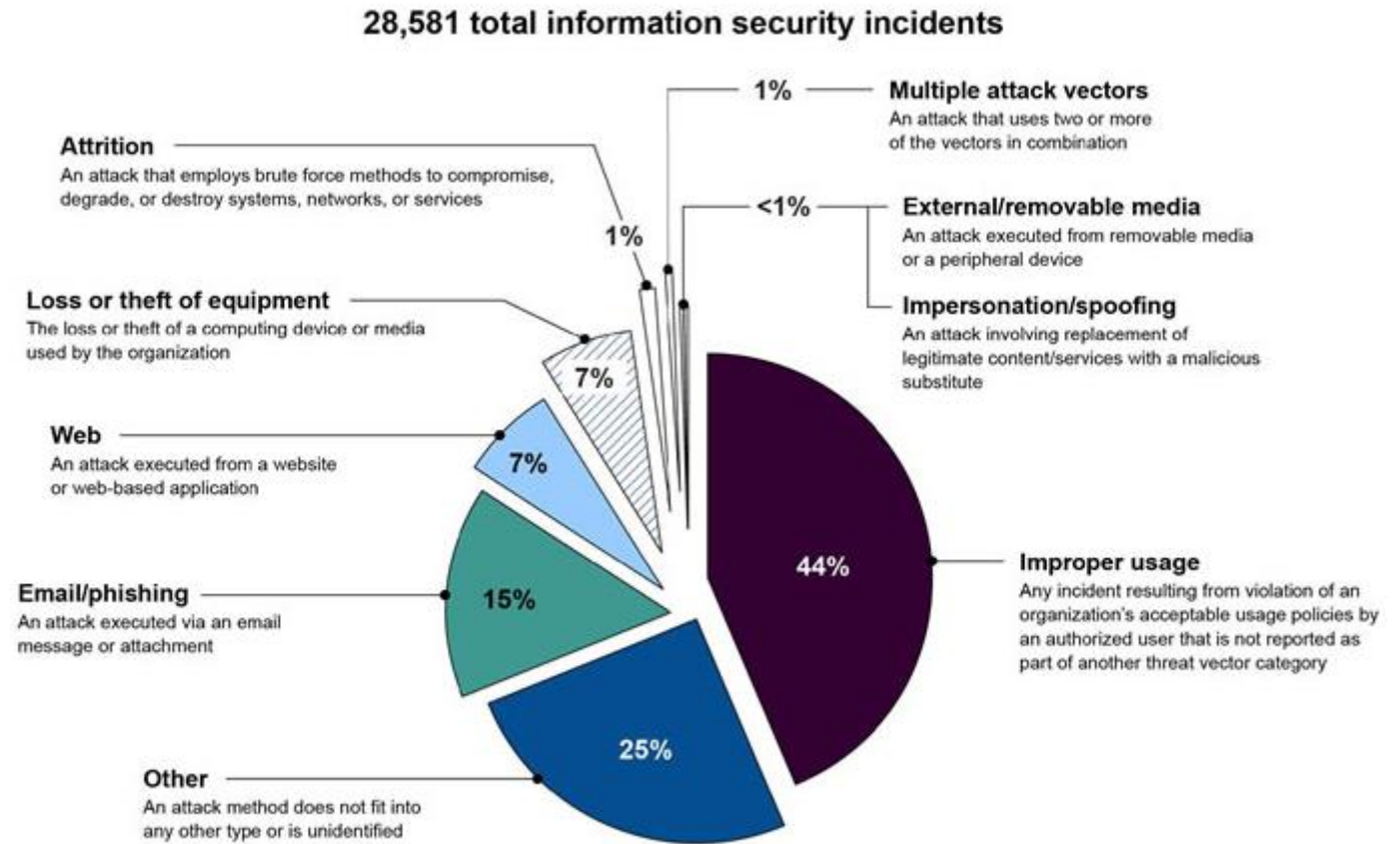
Crime Type by Victim Loss			
Crime Type	Loss Amount	Crime Type	Loss Amount
Advanced Fee	\$5,469,508	Identity Theft	\$4,025,724
BEC/EAC	\$53,190,542	Investment	\$1,862,137
Charity	\$112,717	Lottery/Sweepstakes/Inheritance	\$1,007,503
Civil Matter	\$156,895	Malware/Scareware/Virus	\$36,693
Confidence Fraud/Romance	\$8,032,153	Misrepresentation	\$57,730
Corporate Data Breach	\$709,154	No Lead Value	\$0
Credit Card Fraud	\$2,651,615	Non-payment/Non-Delivery	\$11,218,696
Crimes Against Children	\$0	Other	\$389,877
Criminal Forums	\$0	Overpayment	\$1,418,084
Denial of Service/TDoS	\$180	Personal Data Breach	\$2,822,312
Employment	\$1,132,130	Phishing/Vishing/Smishing/Pharming	\$1,449,437
Extortion	\$5,204,953	Ransomware	\$454,029
Gambling	\$1,981	Re-shipping	\$11,160
Government Impersonation	\$5,605,125	Real Estate/Rental	\$3,838,759
Hacktivist	\$0	Spoofing	\$12,246,482
Harassment/Threats of Violence	\$288,937	Tech Support	\$2,068,844
Health Care Related	\$7,250	Terrorism	\$0
IPR/Copyright and Counterfeit	\$62,684		
Descriptors*			
Social Media	\$2,912,249	Virtual Currency	\$2,470,111

Top Routinely Exploited Vulnerabilities

- Malicious cyber actors are increasingly targeting unpatched Virtual Private Network vulnerabilities
- March 2020 brought an abrupt shift to work-from-home that necessitated, for many organizations, rapid deployment of cloud collaboration services, such as Microsoft Office 365 (O365)
 - Malicious cyber actors are targeting organizations whose hasty deployment of Microsoft O365 may have led to oversights in security configurations and vulnerable to attack
- Cybersecurity weaknesses—such as poor employee education on social engineering attacks and a lack of system recovery and contingency plans—have continued to make organizations susceptible to ransomware attacks in 2020





GAO Report: Federal Agencies

- Over 28,000 security incidents were reported by federal executive branch civilian agencies to the Department of Homeland Security in fiscal year 2019
- Government IT systems contain vast amounts of PII



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal year 2019.

10 Critical Actions Needed to Address 4 Major Cybersecurity Challenges

			
<p>Establishing a comprehensive cybersecurity strategy and performing effective oversight</p>	<p>Securing federal systems and information</p>	<p>Protecting cyber critical infrastructure</p>	<p>Protecting privacy and sensitive data</p>
<p>1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.</p>	<p>5 Improve implementation of government-wide cybersecurity initiatives.</p>	<p>8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).</p>	<p>9 Improve federal efforts to protect privacy and sensitive data.</p>
<p>2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).</p>	<p>6 Address weaknesses in federal agency information security programs.</p>		
<p>3 Address cybersecurity workforce management challenges.</p>	<p>7 Enhance the federal response to cyber incidents.</p>		
<p>4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).</p>			<p>10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.</p>

Source: GAO analysis.

Cybersecurity Adversaries

According to Madeline Mortelmans, Defense Department's Principal Director for Cyber Policy:

- In 2018, the Justice Department estimated that more than 90% of economic espionage cases involved China and more than two-thirds of the cases involved in the theft of trade secrets were connected to China
- Russia is conducting cyber espionage that has the potential to disrupt critical infrastructure and erode confidence in America's democratic system
- North Korea has hacked financial networks and cryptocurrency to generate funds to support their weapons development program
- Iran has conducted disruptive cyberattacks against U.S. and allies' companies, along with information operations to push their own narrative across the Middle East
- Cyber criminals pose a growing threat from their use of ransomware to extort money from local and state governments as well as the commercial sector

Top 5 Cybersecurity Threats

1. *Third-Party and Supply Chain Attacks by Nation-State 'Actors'*
2. Phishing & Social Engineering
3. Malware & Ransomware
4. Data Breaches
5. Insider Attacks

Industry Feedback

- After SolarWinds hack ... the future of nation-states cyber espionage in civilian infrastructure is here
- Information security is an asymmetric warfare (between hackers and their victims), it constantly changes and defies conventional approaches
- Your business has either been hacked or will be hacked – that's a fact
- COVID and 'cloud' ... not the right direction
- Increasing spending and resource allocation ... current, à la carte, reactive, and highly fragmented approaches proved to be ineffective

How do we get ahead of ... ?

Discussion



Questions?



**INNOVATION
COLLABORATIVE
HAMPTON ROADS**

Contact

Tracy Gregorio

CEO

G2 Ops, Inc.

Phone: (757) 965-8330

E-mail: Tracy@g2-ops.com

Dr. Bartosz Wojszczyk

President & CEO

Decision Point Global

Phone: (206) 601-1776

E-mail: Bartosz@dpointg.com