FREE WEBINAR

DR. AMELIA ESTWICK

AGENDA (1-HOUR WEBINAR)

1. HOST & WEBINAR RULES (KEWAL DHARIWAL)
2. WELCOME DAMA (MARC NOLTE, BOB HIEW)
3. SPEAKER INTRODUCTION (BOB HIEW)
4. PRESENTATION (MALCOLM (AMELIA ESTWICK)
5. QUESTIONS (SURINDER PADEM)
6. THANK YOU (ERIC DRESSLER)
WEBINAR RULES

MICROPHONES: MUTED

QUESTIONS: USE CHAT WINDOW
- SURINDER PADEM - MODERATOR FOR QUESTIONS.

WEBINAR: WILL BE RECORDED AND POSTED TO THE DAMA, AND ICCP WEBSITES

WEBINAR FACILITATOR KEVAL DHARIWAL (ICCP)
ICCP CERTIFICATIONS

CERTIFIED CYBER SECURITY PROFESSIONAL
ASSISTANT CYBER SECURITY PROFESSIONAL
1. ASSISTANT — ONE 60-MINUTE EXAM
2. PRACTITIONER — ONE-90-MINUTE EXAM PLUS 2-4 YEARS EXPERIENCE
3. MASTER — ONE 90-MINUTE EXAM, 4 YEARS OF EXPERIENCE, PLUS COACHING-TEACHING-MENTORING COURSE

MORE INFO:
HTTPS://ICCPOG/PROFESSIONALS/EXAMINATIONS.HTML
MEMBERSHIP APPLICATION:
HTTPS://ICCPOG/MEMBERSHIP-APPLICATION.HTML

Hosted by
HTTPS://ICCPOG.ORG

DAMA Edmonton
DAMA Calgary
http://dama-Edmonton.org
iccp
Institute for Certification of Computing Professionals
1. Foundations of Cyber Security (10%)
2. Computer Hacking Forensic Investigators (24%)
3. Ethical Hacking (11%)
4. Incident response handling and disaster recovery (14%)
5. Network Security Administration (17%)
6. Secure Programming issues (14%)
7. Security Analyst (10%)

CYBER SECURITY EXAM CONTENTS
FREE WEBINAR

DR. AMELIA ESTWICK

AGENDA (1-HOUR WEBINAR)

1. HOST & WEBINAR RULES (KEWAL DHARIWAL)
2. WELCOME DAMA (MARC NOLTE, BOB HIEW)
3. SPEAKER INTRODUCTION (BOB HIEW)
4. PRESENTATION (MALCOLM (AMELIA ESTWICK)
5. QUESTIONS (SURINDER PADEM)
6. THANK YOU (ERIC DRESSLER)
Data Security – Assuring Protection for Your Data Sources

Dr. Amelia Estwick
Director of the National Cybersecurity Institute at Excelsior College

Data Management Association - Edmonton
March 25, 2021
Data Security – Assuring Protection for Your Data Sources

Dr. Amelia Estwick
Director of the National Cybersecurity Institute at Excelsior College

Data Management Association - Edmonton
March 25, 2021
Disclaimer

The views and opinions expressed in this presentation are those of the author and does not necessarily reflect the official policy or position of any agency of the U.S. government to include current and former employers.
Speaker: Amelia Estwick

Background: 20+ years Intelligence Community, Government IT, SOC, Cybersecurity, Threat Intelligence, Certified Ethical Hacker, Computer Science Researcher, Adjunct Faculty, The George Washington University Alum, U.S. Army Gulf-War Veteran, National Physical Sciences Consortium Fellow and ..........a little paranoid!
## Global Risk Report 2021

### Top Risks by likelihood
1. Extreme weather
2. Climate action failure
3. Human environmental damage
4. Infectious diseases
5. Biodiversity loss
6. Digital power concentration
7. Digital inequality
8. Interstate relations fracture
9. Cybersecurity failure
10. Livelihood crises

### Top Risks by impact
1. Infectious diseases
2. Climate action failure
3. Weapons of mass destruction
4. Biodiversity loss
5. Natural resource crises
6. Human environmental damage
7. Livelihood crises
8. Extreme weather
9. Debt crises
10. IT infrastructure breakdown

## Total Data Records Lost or Stolen by Country

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>6,219,819,956</td>
</tr>
<tr>
<td>India</td>
<td>394,307,531</td>
</tr>
<tr>
<td>China</td>
<td>350,752,955</td>
</tr>
<tr>
<td>South Korea</td>
<td>228,726,843</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>140,139,193</td>
</tr>
<tr>
<td>Turkey</td>
<td>132,312,866</td>
</tr>
<tr>
<td>Japan</td>
<td>114,769,575</td>
</tr>
<tr>
<td>South Africa</td>
<td>106,654,166</td>
</tr>
<tr>
<td>France</td>
<td>100,099,535</td>
</tr>
<tr>
<td>Mexico</td>
<td>98,252,295</td>
</tr>
<tr>
<td>Canada</td>
<td>91,830,959</td>
</tr>
<tr>
<td>Russia</td>
<td>56,740,681</td>
</tr>
<tr>
<td>Australia</td>
<td>50,342,722</td>
</tr>
<tr>
<td>Malaysia</td>
<td>46,347,351</td>
</tr>
<tr>
<td>Germany</td>
<td>44,887,197</td>
</tr>
<tr>
<td>Taiwan</td>
<td>35,414,686</td>
</tr>
<tr>
<td>Iran</td>
<td>23,562,000</td>
</tr>
<tr>
<td>Spain</td>
<td>11,159,702</td>
</tr>
<tr>
<td>Pakistan</td>
<td>10,748,176</td>
</tr>
<tr>
<td>Serbia</td>
<td>7,276,605</td>
</tr>
<tr>
<td>Ukraine</td>
<td>7,000,000</td>
</tr>
<tr>
<td>Denmark</td>
<td>6,203,195</td>
</tr>
<tr>
<td>Sweden</td>
<td>6,174,257</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>4,422,998</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>3,504,000</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>2,832,312</td>
</tr>
<tr>
<td>Netherlands</td>
<td>1,927,479</td>
</tr>
<tr>
<td>New Zealand</td>
<td>1,686,928</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Italy</td>
<td>862,218</td>
</tr>
<tr>
<td>Vietnam</td>
<td>735,000</td>
</tr>
<tr>
<td>Ireland</td>
<td>382,899</td>
</tr>
<tr>
<td>Chile</td>
<td>308,189</td>
</tr>
<tr>
<td>Brazil</td>
<td>285,373</td>
</tr>
<tr>
<td>Kenya</td>
<td>134,000</td>
</tr>
</tbody>
</table>

**Total Data Records Lost or Stolen Since 2013:** 9,727,967,988

Source: https://www.varonis.com/blog/the-world-in-data-breaches/
Cost of a Data Breach

Global average total cost of a data breach in 2020

$3.86M

- Healthcare has the highest industry average cost.
- Customer PII data has the highest cost per record.
- United States has the highest country average cost.

CYBERCRIME is estimated to cost the world $6 TRILLION annually by 2021.

It is predicted that GLOBAL CYBERSECURITY spending will exceed $1 TRILLION cumulatively from 2017 to 2021.

Sources:
Information Security and Privacy in the Times of COVID-19

- 92% say threat actors will increase cyberattacks on individuals.
- 87% say rapid shift to work from home increased risk of data privacy and protection issues.
- 58% say threat actors will take advantage of the pandemic to disrupt organizations.

Only 51% are highly confident in their security team’s ability to detect and respond to these cyberthreats during the pandemic.

Methods of Data Breaches

Theft or unauthorized disclosure of personal information

- Hacked
  - Ransomware
  - Malware
  - Phishing
  - Denial-of-Service
- Payment card
- Poor security/Error
- Insider Threat
- Lost device/Misuse

Source: Dataversity
Ransomware + Pandemic = Chaos

Source: https://www.blackfog.com/the-state-of-ransomware-in-2021/
Increase in PYSA Ransomware Targeting Education Institutions

Summary

FBI reporting has indicated a recent increase in PYSA ransomware targeting education institutions in 12 US states and the United Kingdom. PYSA, also known as Mespinoza, is a malware capable of exfiltrating data and encrypting users’ critical files and data stored on their systems. The unidentified cyber actors have specifically targeted higher education, K-12 schools, and seminaries. These actors use PYSA to exfiltrate data from victims prior to encrypting victim’s systems to use as leverage in eliciting ransom payments.

IoT Devices Connected Worldwide

- 2020 World population ~ 8 Billion
- 2020 IoT Devices ~34 Billion

THAT'S MORE THAN 4 DEVICES FOR EVERY HUMAN ON EARTH

What is Metadata?

Data that provides information about other data. Information that is generated as you use technology and that lets you know the who, what, where, when and how of a variety of activities.

Where does it come from?

- Making a phone call:
  - Phone number of caller
  - Phone number(s) called
  - Unique serial numbers of phones involved
  - Time of call
  - Duration of call
  - Location of each participant
  - Telephone calling card numbers

- Internet Browsing:
  - Pages visited and when
  - User data and possibly user login details with auto-fill features
  - URLs
  - Your IP address, Internet service provider, device hardware details, operating system and browser version
  - Cookies and cached data from websites
  - Your search queries
  - Results that appeared in searches
  - Pages you visit from search
  - Your name and profile biographical information including birthday, hometown, work history and interests

- Sending an E-mail:
  - Sender's name, email and IP address
  - Recipients' name and email address
  - Server transfer information
  - Date, time and timezone
  - Unique identifier of email and related emails (Message-ID)
  - Content type and encoding
  - Mail client login records with IP address
  - Mail client header formats
  - Priority and categories
  - Subject of email
  - Status of the email
  - Read receipt request

- Social Networking:
  - Your username and unique identifier
  - Your subscriptions
  - Your location
  - Your device
  - Activity date, time and timezone
  - Your activities, "likes", check-ins and events
  - Language
  - When you created your account
  - Tweet's location, date, time and timezone
  - Tweet's unique ID and ID of tweet replied to
  - Contributor ID
  - Your followers, following and favorite count
  - Your verification status
  - Application sending the tweet

What can it reveal?

Metadata is...

"Arguably more revealing [than content] because it's actually much easier to analyze the patterns in a large universe of metadata and correlate them with real-world events than it is to go through a semantic analysis of all of someone's email and all of someone's telephone calls."

- Daniel Weitzner
  - Computer scientist

And so...

In many cases, courts have recognized that metadata can reveal much about an individual and deserves privacy protection, while recognizing that context matters.

Source: www.priv.gc.ca/media/2345/md_info_201410_e.pdf
1. THE RAPID GROWTH OF GLOBAL DATA

The production of data is expanding at an astonishing pace. Experts now point to a 4300% increase in annual data generation by 2020. Drivers include the switch from analog to digital technologies and the rapid increase in data generation by individuals and corporations alike.

2012: CUSTOMERS WILL START STORING 1 EB OF INFORMATION.

DATA PRODUCTION WILL BE 44 TIMES GREATER IN 2020 THAN IT WAS IN 2009

More than 70% of the digital universe is generated by individuals. But enterprises have responsibility for the storage, protection, and management of 80% of it.

WHAT IS A ZETTATYPE?

1,000,000,000,000,000 gigabytes
1,000,000,000,000 terabytes
1,000,000,000 petabytes
1,000,000,000 exabytes
1,000,000,000 zettabytes

Source: https://digitalguardian.com/blog/history-data-breaches
The solution lies in distilling billions of events into hundreds of anomalies, then into a handful of actionable SOC leads.


ANALYTICS + AI + MACHINE LEARNING
Top 5 Cybersecurity Investments Since Beginning of Pandemic

Ranked by % selected among Total

- Multi-factor authentication (MFA): 20%
- Endpoint device protections: 17%
- Anti-phishing tools: 16%
- VPN: 14%
- End-user security education: 12%

Top 5 Cybersecurity Investments Since Beginning of Pandemic

Ranked by % selected among Total

- Multi-factor authentication (MFA): 20%
- Endpoint device protections: 17%
- Anti-phishing tools: 16%
- VPN: 14%
- End-user security education: 12%

CYBER SAFETY CHECKLIST

- Back up online and offline files regularly and securely
- Strengthen your home network
- Use strong passwords
- Keep your software updated
- Manage social media profiles
- Check privacy and security settings
- Avoid opening and delete suspicious emails or attachments

Source: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats
Basic Cyber Hygiene

✓ Culture of cyber awareness

Source: https://surfshark.com/
Basic Cyber Hygiene

- Culture of cyber awareness
- Use strong passwords/multi-factor authentication (MFA)
- Change account passwords frequently
- Check/Update privacy settings in social media accounts - 90 days
- Use a Virtual Private Network (VPN)

Source: https://surfshark.com/
MOBILE DEVICE SECURITY

1. Password Protect Your Device
2. Lock Your Screen
3. Encrypt It
4. Limit Password Attempts
5. Use Anti-Malware Software
6. Don’t Jailbreak or Root Your Device
7. Be Selective With Apps
8. Limit App Permissions
9. Keep Software Up-To-Date
10. Limit Location Information
11. Review Voice Commands
12. Promptly Report Lost/Stolen Devices
13. Bluetooth, Wifi & NFC
14. Safely Dispose of Your Device
15. Consider Using Find My Phone

Source: https://www.integriscu.ca/mobile-device-security-top-tips/
Mobile Device Best Practices

- Always apply system updates
- Regularly check for app updates
- Don’t install apps you didn’t go looking for
- Remove/uninstall apps you are no longer using
- Check the app permissions before installing
- Avoid click-bait (text messages)
Mobile Device Best Practices

✓ Always apply system updates
✓ Regularly check for app updates
✓ Don’t install apps you didn’t go looking for
✓ Remove/uninstall apps you are no longer using
✓ Check the app permissions before installing
✓ Avoid click-bait (text messages)

✓ If you have mobile banking
  ✓ Protect with multi-factor authentication
  ✓ Set up alerts via email, text or the bank’s app
✓ DO NOT USE public Wi-Fi
Enterprise Security Solutions

✓ Culture of cyber awareness
✓ Zero Trusts
✓ Security Information and Event Monitoring (SIEM)
✓ Security Orchestration Automation and Response (SOAR)
✓ Identity and Access Management (IAM)
✓ Managed Security Services Provider (MSSP)
Enterprise Security Solutions

- Continuously monitor networks and backup data
- Actively manage all software & devices on the network
- Patch management, update anti-virus/malware
- Employ behavioral, anomaly detection
Enterprise Security Solutions

- Continuously monitor networks and backup data
- Actively manage all software & devices on the network
- Patch management, update anti-virus/malware
- Employ behavioral, anomaly detection
- Risk Management
- Governance, Risk, Compliance (GRC)
- Security Incident Response & Business Continuity Plans

✓ Report suspicious activity!!!!
Q & A

Dr. Amelia Estwick
Director, National Cybersecurity Institute
Excelsior College
7 Columbia Circle
Albany, NY 12203-5159


THANK YOU
BE SAFE STAY VIGILANT