SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

Data Privacy and Data Protection in the COVID Era

Live Webcast

January 20, 2021

10:00 am PT

Today’s Presenters

Alex McDonald
Moderator
Independent Consultant
Chair SNIA CSTI

Mounir Elmously
Senior Manager,
Consulting Services
EY

Eric Hibbard
CISSP, CIPT, CISA
Chair, SNIA Security Technical Working Group

SNIA Legal Notice

- The material contained in this presentation is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

SNIA-At-A-Glance

185
industry leading organizations

2,000
active contributing members

50,000
IT end users & storage pros worldwide

SNIA. CSTI | CLOUD STORAGE TECHNOLOGIES

What We Do

Educate vendors and users on cloud storage, data services and orchestration

Support & promote business models and architectures: OpenStack, Software Defined Storage, Kubernetes, Object Storage

Understand Hyperscaler requirements Incorporate them into standards and programs

Collaborate with other industry associations

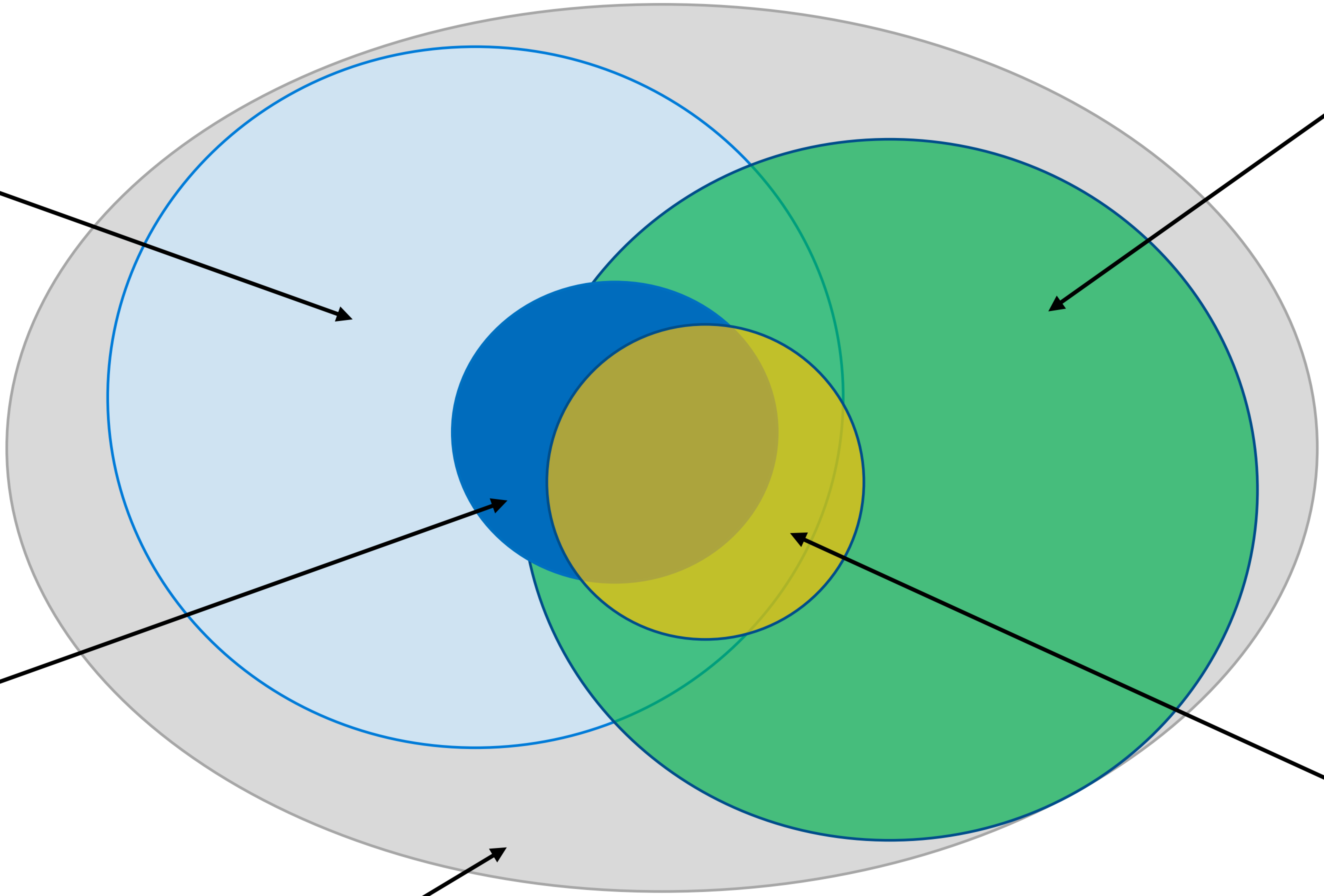
Agenda

- Changing threat landscape
  - Responses to COVID-19
  - Malware
  - Ransomware
- Data protection strategies
  - Why protect data
  - Why backup is not an archive
  - How to protect date

Changing Threat Landscape

Eric Hibbard

When staying safe means more than just washing your hands.



Privacy: Collection Limitations, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability

Information Security: Ensures Confidentiality, Integrity, and Availability (CIA) of information

Personal Data Protection: Safeguards applying under various laws and regulations to personal data (PII, PHI, etc.) about individuals that organizations collect, store, use and disclose

Ethics: Moral principles that govern a person's behavior or the conducting of an activity

Cybersecurity: Ensures Confidentiality, Integrity, and Availability of data; Identify, Protect, Detect, Respond, Recover

Current Threat Landscape (Order of Prevalence)

- Social Engineering
- Advanced Persistent Threat (APT)
- Ransomware/Malware
- Unpatched/Updated Systems
- Security Misconfiguration
- Denial of Service
- Sensitive Data Exposure
- Injection Flaws
- Cryptojacking
- Cyber Physical Attacks
- Broken Authentication
- Broken Access Control
- Third Party (Supplier)
- Insider Theft
- Mobile Malware
- Physical Loss of Devices
- Cross-site Scripting (XSS)
- Man-in-the-Middle Attacks
- IoT Weaponization

Additional Attacker Exploits For the COVID-19 Crisis

- Phishing emails
- Malicious apps
- Bad domains
- Insecure endpoints and end users
- Vulnerabilities at vendors and third parties
- Communications apps and working from home
- Targeting healthcare organizations and COVID hotspots
- Exploiting future fallout and recovery

FBI's COVID-19 Response

- **Crimes Against Children**
  - Criminals broadcast child sexual abuse material to unwitting participants of school, church, or other online gatherings
  - Sexual predators victimizing children or teens in sextortion schemes as children spend more time online and out of school
- **Fraud**
  - Government Impersonators
  - Fraudulent Cures (Vaccine) or Medical Equipment
  - Work-from-Home Fraud
  - Investment Fraud
  - Unemployment insurance and the Paycheck Protection Program
  - Charity Scams

CISO Responses to COVID-19

- Big security projects have been postponed indefinitely
- Securing remote users
  - Executives mandates – get employees up and running first and then address security afterward
  - “Bolt on” security is the order of the day; requires collaboration with IT/network operations
- Finding and patching holes as quickly as possible
- Security teams are robbing Peter to pay Paul, grabbing money as they can to address the new reality

CISO Responses to COVID-19 (cont.)

- Endpoint security controls – focus is on providing network access and blocking malware
- Mobile device security – executives, high-value employees, and privileged account managers are working from home
- Network security – VPNs and Zero Trust access; interest in secure DNS
- Simple multi-factor authentication (MFA)
- End-user monitoring

Combating Malware

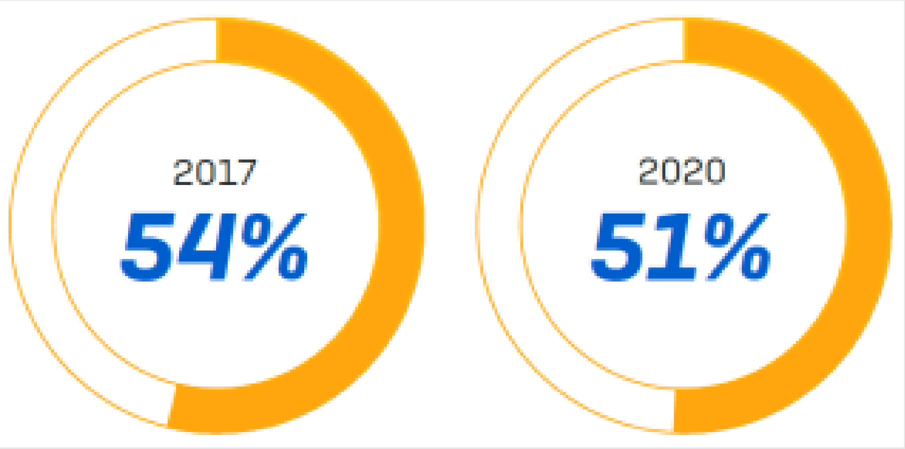
- Patch/Update OS, browsers, plugins, etc. regularly
- Update all application software regularly
- Use all the necessary security tools (antivirus software)
- Stay alert for social engineering attacks (phishing emails)
- Never click on links or download attachments coming from untrusted on unknown sources

Combating Malware (cont.)

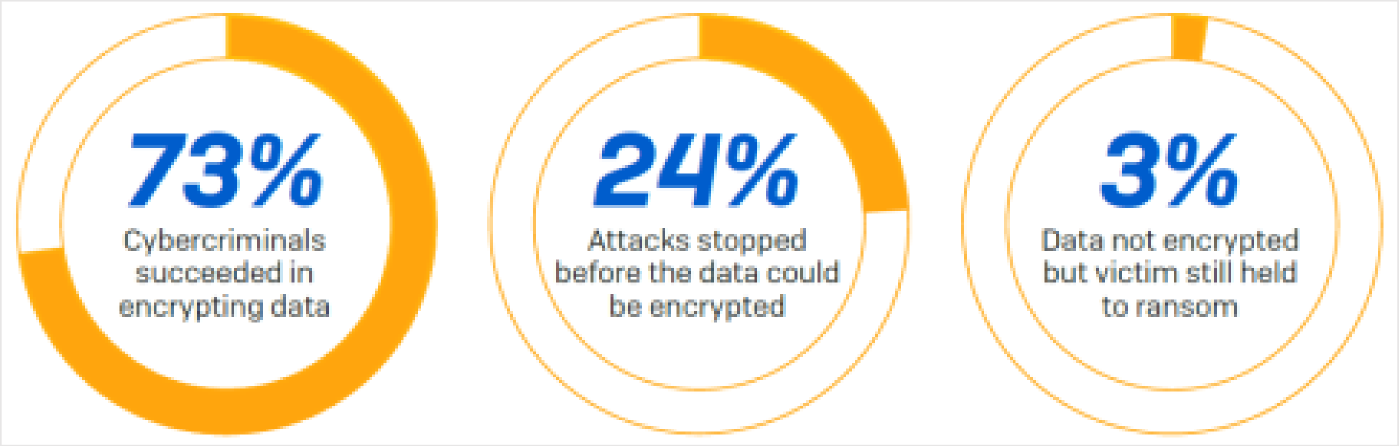
- Practice safe browsing
- Have strong passwords, change passwords periodically
- Refrain from using un-encrypted public connections
- Layer your security starting with basic measures like firewall and antivirus

Ransomware Statistics

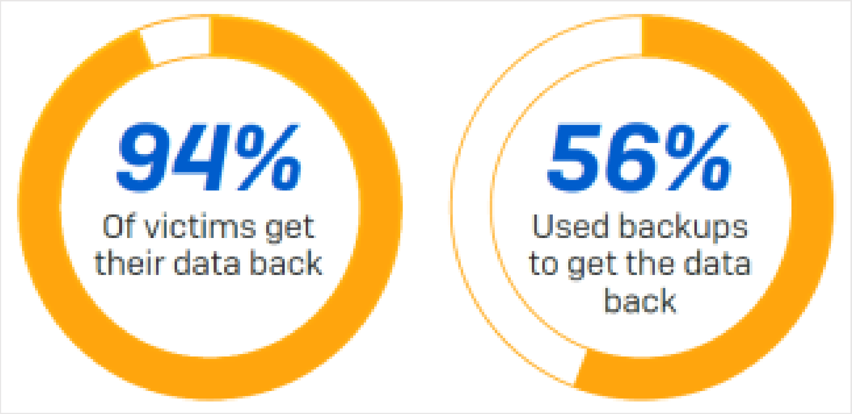
Prevalence of Ransomware



Impact of Ransomware



Getting Data Back



Source: *Sophos.*

Minimizing Ransomware Risks

- Start with the assumption that you *will* be a victim
- User education and training (phishing and social engineering)
- Minimize attack surface by patching vulnerabilities, antivirus updates, and disabling unnecessary services (like RDP)
- Invest in anti-ransomware technology to stop unauthorized encryption (e.g., endpoint monitoring and protection)

Minimizing Ransomware Risks (cont.)

- Protect data wherever it’s held (public cloud, private cloud, and on premises)
- Make regular/automated backups and store offsite and offline
- Have an incident response plan that addresses ransomware
- Ensure your cyber insurance covers ransomware
- Deploy a layered defense; defend against all vectors of attack

Data Protection Strategies

Mounir Elmously

Data Protection

What is data? How different is it from information?

Why protect data?

What is data protection?

What Data Protection is NOT?

Why isn’t Backup an Archive

How to protect data?

What Is Data?
How Different Is It From Information?

- Industry definition of data: "The representation of anything in any form that is unprocessed"
  - Social security number, driver's license number, passport number, etc. when not associated with definition
- Data can be in hardcopy format
  - Papers, photos, videos, etc.
- Data can be digital in binary format
  - Data stored on disk, tape, cloud)
- Data can be structured or unstructured and can exist in many forms
  - Numbers, words or symbols and can relate to transactions, events or facts but is not generally very useful until it is processed into information.

What Is Data?
How Different Is It From Information?

- Industry definition of information:
  - Information is processed data
  - It has meaning and context
  - Not just a single data point
  - A series of data points that have been interpreted within a context, such as an application, or processed in such a way as to be meaningful to the person who receives it.

Why Protect Data?

- Since humanity has learned to store information, it realized that stored information is subject to
  - Data loss partially or totally
  - Media failure (e.g. fire, floods, natural disasters, etc.)
  - Corruption
  - Inadvertently or intentionally changed
  - Pandemics and plaques that historically wiped a considerable portion of human legacy
- Even when Egyptians learned to store information in stones, they soon realized that stone inscription is not eternal
- Hence the need to protect information has always been an integral component of information preservation

What is Data Protection?

- Data protection is the process of creating copies of digital data stored on an independent media to ensure access to stored contents even when the original data is no longer available or accessible (hardware failure, accidental deletion, ransomware, etc.)
- Some data protection methods may be subject to the same risks of the original contents.
- Historically, removable storage disks were used to protect data copies that were portable and provide adequate isolation from original data
- Removable disks have been subject to severe reliability issues that soon were abandoned in favor tape

What Data Protection Is NOT

- For multiple decades, the IT industry had only two data storage options
  - Disk (relative high cost) high performance that provides fast access to stored data but subject to many risks that may result in data loss depending on the nature of the data loss event
  - Tape (relative low cost) provides adequate isolation from original data both physically and logically
- In addition to transactional data and backups, organizations had distinct need to maintain information **archive**. This led to simply consider the backup as archive

Why Isn’t Backup an Archive?

- With legacy technologies that dominated the market, all data storage systems were controlled by the same vendor, which provided limited or no change to backed up data.
- Coupled with limited data volumes and less stringent regulatory requirements, backup was meeting archiving requirements
- With the introduction of open systems and cloud technologies coupled with exponential data growth, these changes have influenced the archive industry
  - Multiple storage technologies with plethora of cost, performance and availability options
  - Faster update cycles for operating systems, backup technologies with even faster pace for media upgrades with limited or no backward compatibility
- This resulted that for extended retention, chances are that backups cannot be read and even if it can, response to regulatory investigation will not meet time constraints

How to Protect Data?

- Creating copies of data may take any of the following forms:
  - Data cloning
  - Snapshots
  - Backup to disk, tape, or the cloud
  - Replication
  - Air gap storage solutions

- Despite that snapshots and replication are lightweight data copies, that provide much faster access to protected data, they typically do not protect from all data loss scenarios, organizations should employ multiple data protection methods to address varying data loss scenarios while meeting data availability requirements.

How to Protect Data?

- Air gap storage solutions have recently gained momentum due to the increased sophistication of cyber threats.
- Typically implemented as a duplicate copy of backup data on a secondary storage system that is offline and thus not connected to any production or public networks.
- The air gap storage solution provides an additional data set that is immune from malware manipulation.

Data Protection During a Pandemic

- Pandemic has created an unprecedented remote work and BYOD shift.
- Very likely that written policies and procedures in comprehensive information security programs are not being followed or enforced.
- There is case law indicating that failure to consistently follow a retention policy is worse than not having a written policy at all.
- Understandably, many privacy compliance obligations are immutable, but if organizations were not able to monitor or enforce its pre-Covid policies, they should at least investigate the gaps. Gaps can be prioritized based on risk.

Data Protection During a Pandemic (cont.)

- Luckily, under law this kind of self-own can be kept confidential if the organization has the foresight to conduct such review under the protection of attorney-client and work product protections.
- It might be prudent to put in writing a set of emergency guidelines based on those priorities.
- If something happens it is usually too late. Litigators and investigators have a right to request production of or subpoena BYOD devices.

Final Thoughts

- Adversaries are changing their attacks at a rapid pace; defenders must be nimble
- Data is today’s currency; adversaries can prosper by using your data or by depriving you of your own data
- People (especially children) continue to be the weak link
- Emerging technologies (5G, IoT, AI, etc.) will expand the threat landscape
- Reasonable security and due care expectations on the rise with severe consequences for inadequate responses

Q&A

After This Webcast

- Please rate this webcast and provide us with feedback
- This webcast and a copy of the slides will be available at the SNIA Educational Library https://www.snia.org/educational-library
- A Q&A from this webcast will be posted to the SNIA Cloud blog: www.sniacloud.com/
- Follow us on Twitter @SNIACloud

References

- On-Demand Webccast:s: Storage Networking Security Series
  - Understanding Storage Security & Threats
  - Encryption 101
  - Key Management 101
  - Applied Cryptography
  - Protecting Data at Rest
  - Protecting Data in Transit
  - Security & Privacy Regulations
- Article: Data Protection in an Era of Massive Data Breaches
- Blog: Data Aggregation during a Pandemic
- Blog: Addressing Cloud Security Threats with Standards
- On-Demand Webcast: Cloud Standards: What They Are, Why You Should Care

Thank you!