Keenan®

Expect The Unexpected

Lessons Learned in Cyber

PARMA 2024

Who is Keenan & Associates?

Keenan provides innovative insurance and financial solutions for schools, public agencies, and health care organizations. We serve those who support our communities. Our high quality, cost effective programs exceed our customers' expectations. Experts that you can relay on when it comes to employee benefits, risk management, JPA management and claims services.

Disclaimer

Keenan & Associates is an insurance brokerage and consulting firm that provides risk management services. It is not a law firm. We do not give legal advice and neither this training presentation, the answers provided, nor the documents accompanying this presentation constitutes or should be construed as legal advice. Clients are advised to consult with their own attorney for a determination of their legal rights, responsibilities and liabilities, including the interpretation of any statue or regulation, or its application to client's business activities.

Today's Panelists

Shawnee Nishimura

- Works with 40+ school districts spanning from Santa Cruz Co., San Benito Co, Lake Co, Mendocino Co, Humboldt and Del Norte Co.
- Manages three property and liability K-12 joint power authorities (JPAs) and two workers' compensation K-12 JPAs and previously a Risk Manager for a Large K-12 School District in Northern California.
- Maintains Fire & Casualty Brokers License and CSRM designation.

Jessica Blushi

- Vice President of the Property & Casualty Marketing at Keenan
- Specializes in reinsurance, self-insurance and risk management.
- Oversees placement and service of a cyber program for over 500 public school districts.

Kiley Heath

- Risk Manager for Mendocino County Office of Education; supporting safety and compliance for twelve K-12 districts.
- Develops and maintains programs which support staff and student safety focusing on both workers' compensation and liability matters.
- Experience in organizing a cyber task force and navigating the County Office through a cyber attack.

Today's Panelists

John Loyal, Esq.

- Partner at Cipriani & Werner and co-chair of the firm's cyber security, Information Privacy and Data Security team focusing primarily on cyber and privacy matters.
- Serves as breach counsel to companies of varying market segments, providing guidance and legal counsel to impacted entities.
- Prior to joining the firm, managed cyber claims for a leading cyber insurance carrier.

Bill Hardin

- Vice President at Charles River Associates, leading global consulting firm.
- Has handled all types of ransomware, data extortion, business email compromise, nation state attacks, malware outbreaks, insider threats, amongst other items.
- CPA, Certified Fraud Examiner (CFE), and Certified Project Management Professional (PMP).

What This Session Will Cover

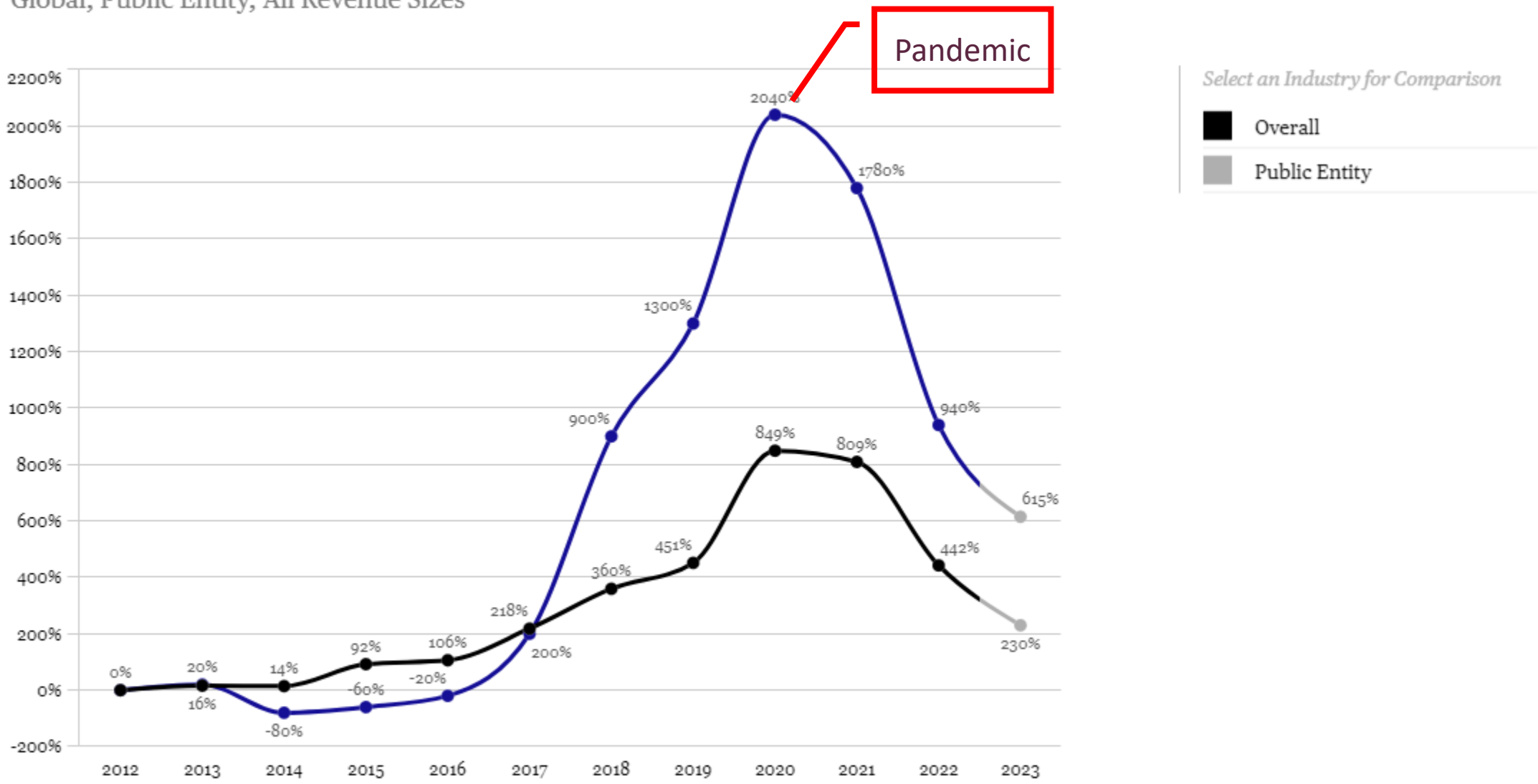
- Cyber Trends
- Cyber Incident Response Process
- Exploring the Dark Web
- Lessons Learned

Cyber Vocabulary

- Cyber Incident
  Compromise, infection, theft, loss or damage to data, a computer system or software.
- Phishing
  Use of personal information and/or a seemingly legitimate or known email address to trick an internal actor.
- Ransomware
  Malware that locks the software and data content of a computer system.
- Actors
  Internal, External, Partner, Threat, Unknown
- Hacking
  Obtaining of unauthorized or criminal access to or control of a computer system, server or network.
- Breach
  Sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by unauthorized actor.
- Malware
  Malicious software, script, or code that is designed to run, alter or change a program or cause a cyber incident.

Global Incident Growth Compared to 2012*

Global, Public Entity, All Revenue Sizes

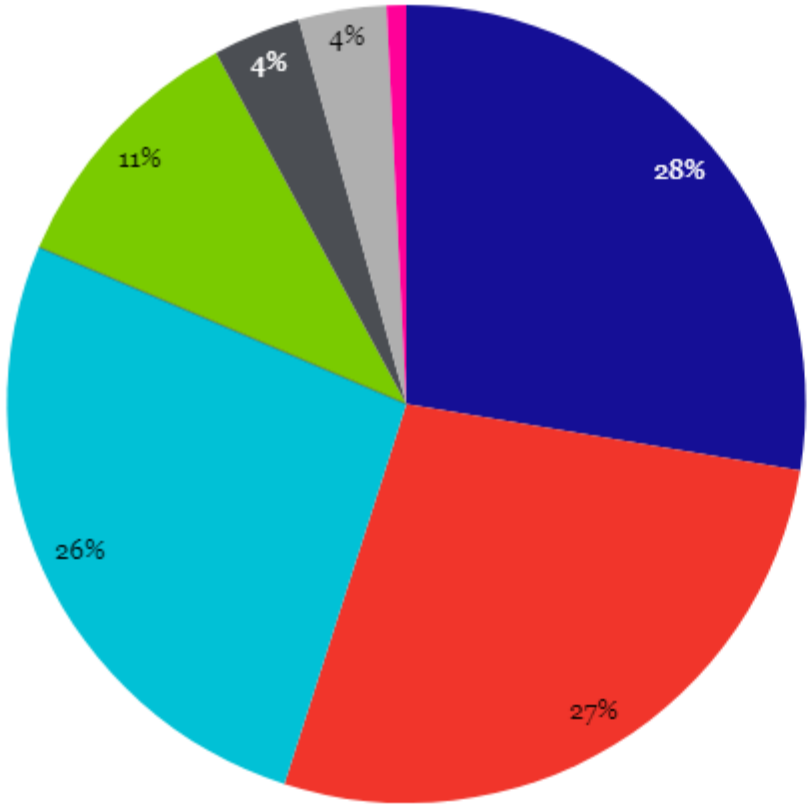


* Please note - this data is indexed against the base line year of 2012 and current year shown in grey is a projection.

CHUBB®

Actions Causing Cyber Incidents - Last Three Complete Years

Global, Public Entity and All Revenue Sizes

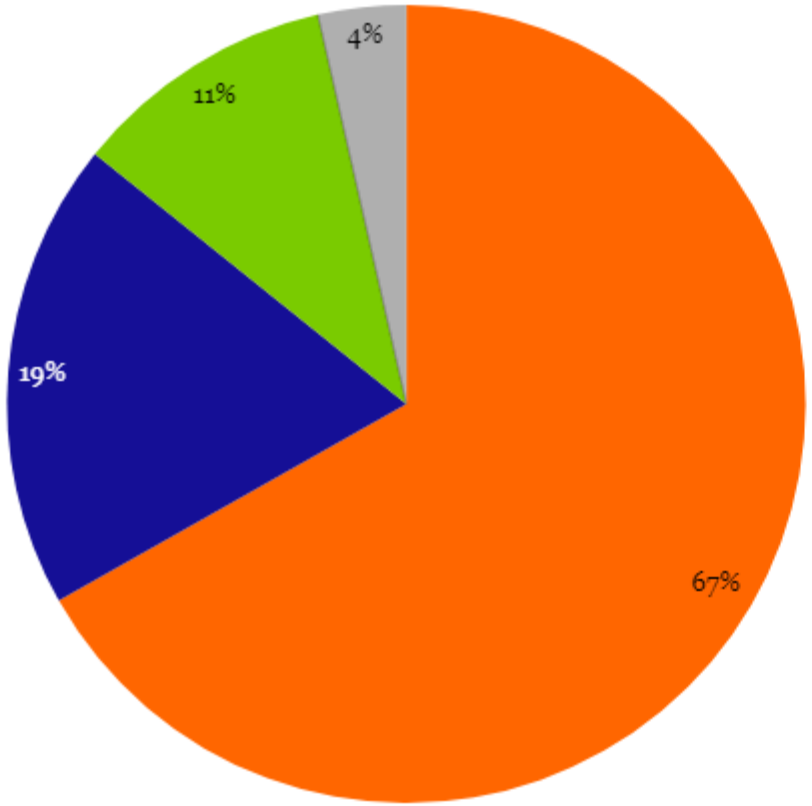


Your Selections vs. Overall	
Error	2% ▲
Hacking	6% ▲
Malware	2% ▼
Misuse	2% ▼
Physical	2% ▼
Social	0% ▲
Unknown	1% ▼

CHUBB®

Actors Causing Cyber Incidents - Last Three Complete Years

Global, Public Entity and All Revenue Sizes



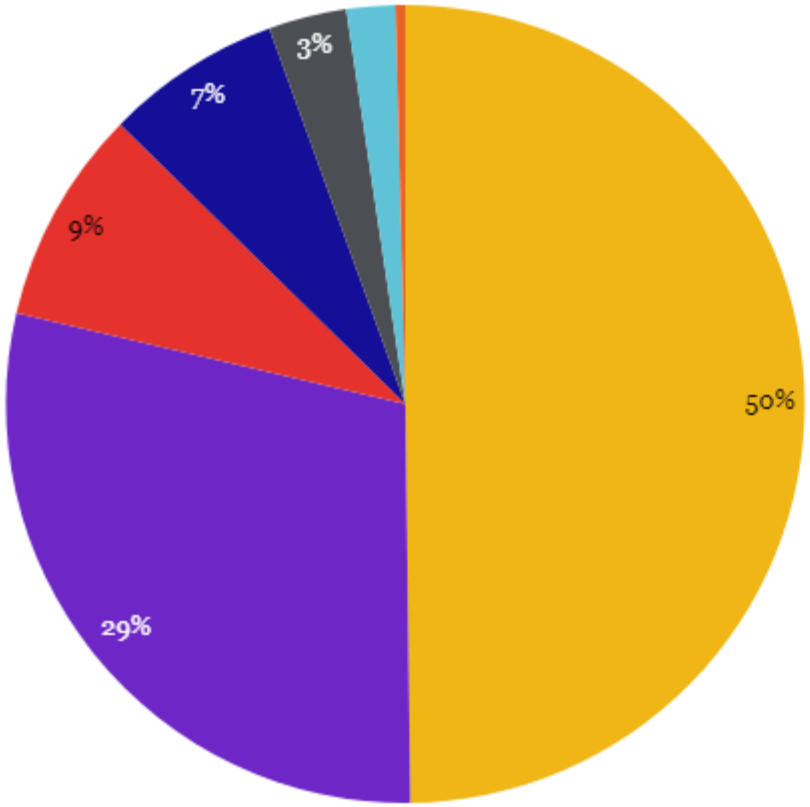
Your Selections vs. Overall

External	2% ▼
Internal	2% ▼
Partner	5% ▲
Unknown	1% ▼

CHUBB®

Assets Affected by Cyber Incidents - Last Three Complete Years

Global, Public Entity and All Revenue Sizes



Your Selections vs. Overall

Media	0%	▲
Network	1%	▲
People	3%	▼
Public Terminal	0%	▼
Server	2%	▲
Unknown	1%	▲
User Device	1%	▼

CHUBB®

Cyber Incident Reporting Process

There's a Cyber Incident – Now What?

Agency Suffers An Incident

Immediately Contact Breach Counsel/Hotline

Incident Response

Claim Reporting

Recovery

Breach Counsel will help the agency determine appropriate third-party vendors to contain the incident and support the member in the recovery of the their business activities

Before you

Blow-out systems in an attempt to restore

Respond to threat actor communications

Make a public statement

Report to authorities

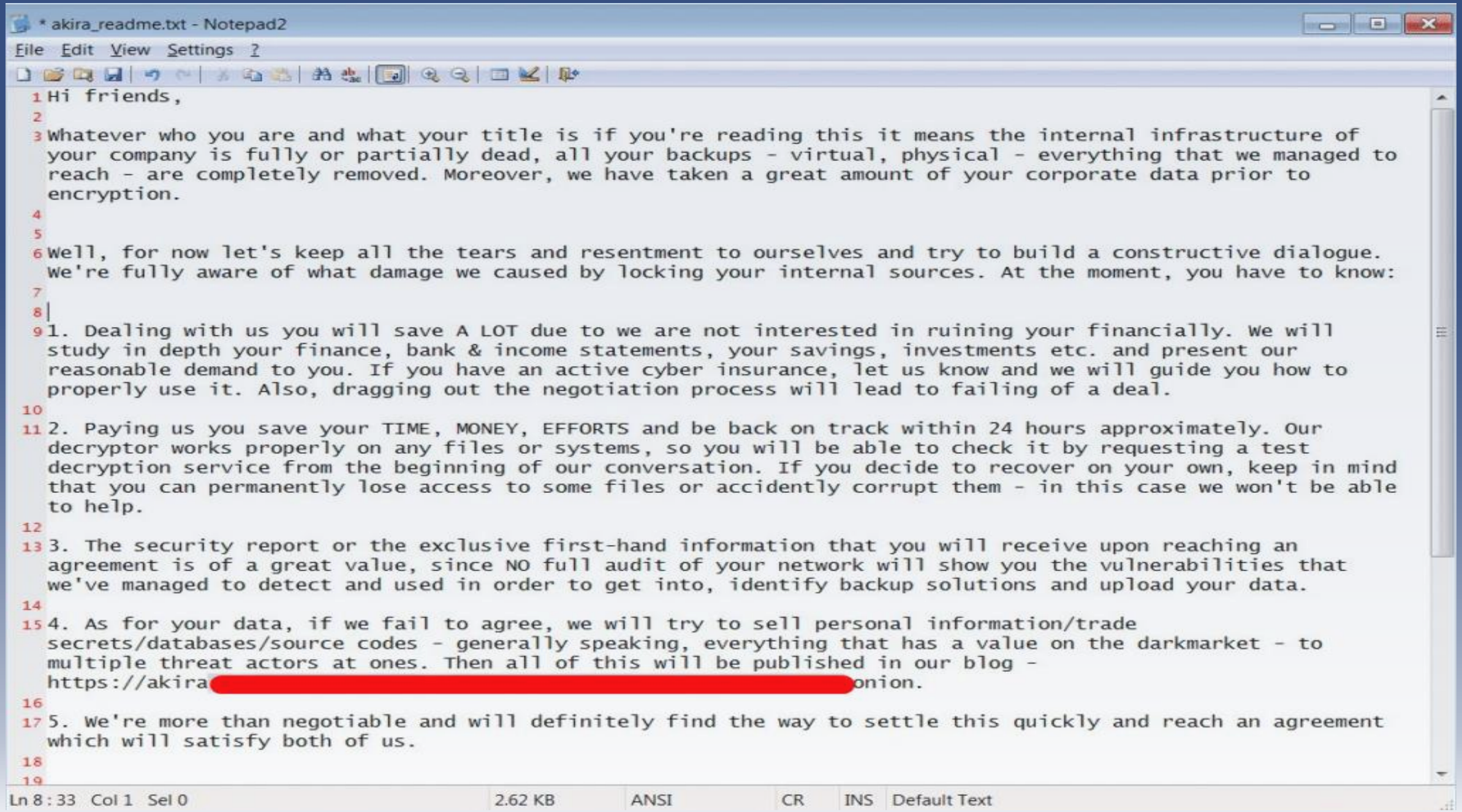
What is a Breach Coach?

Quarterback

Coordinator

Counselor


Available IR Assets
Forensics
Public relations
IR support personnel
Bitcoin wallets
International counsel (if needed)
Forensic accountants
Credit reporting
Mass publication


* akira_readme.txt - Notepad2
File Edit View Settings ?
Hi friends,
Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.
Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:
1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidently corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - https://akira[redacted]onion.
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.
Ln 8 : 33 Col 1 Sel 0
2.62 KB
ANSI
CR
INS
Default Text

WHAT IS RANSOMWARE?

A type of malware that takes control over a computer or computer system by encrypting all the data on the drive.

The data is then held at ransom until a predetermined cost is paid or the affected entity is able to restore from available backups

Due to the use of cryptocurrencies (i.e. bitcoins) for payment, it is difficult to track those demanding the ransom.

RANSOMWARE FACT SHEET

In March 2022, the FBI issued a stark warning to local US governments and public services; ransomware attacks against regional and local governments were disrupting operational services, posing risks to public safety and general financial losses (Source – Knowb4)

When you are impacted by Ransomware – two things will happen

A large number of ransomware matters are not publicly reported. Based on available figures, there was at least a 37% increase in ransomware for 2023 concerning public / local municipalities and nearly a 90% increase for educational institutions. Other than healthcare, education and local municipalities are the two most targeted segments by threat actors.

1) Your systems will be encrypted and your day-day operations will be impacted. Depending on the severity of the incident, employees are often sent him as daily job functions cannot be performed

2) The threat actor will exfiltrate significant amounts of data from your system and will threaten to leak or post this data in the public realm if the ransom is not paid. If you do not pay the ransom – you need to expect that your data will be leaked

Initial ransom demands are now averaging in excess of $1.5M. We can typically negotiate with the threat actors if payment is required.

Do we pay and who decides on the amount?

- Who engages the TA and how are ransom negotiations handled
- How is payment made
- OFAC check
- “Honor among thieves”

The Dark Web

Lessons Learned

Overview of the MCOE Cyber Breach

- Saturday March 4th installed security update for VMware
- Sunday March 5th DNS/DHCP, FileServe, AD not accessible
- Monday March 6th reset admin login to VMware discovered all files were encrypted

  …except one text file with a message from threat actor

#1 CALL YOUR INSURANCE CARRIER

Contact your insurance carrier immediately when there is a cyber breach or suspected cyber breach.

Communication

~~There's no such thing as "too much" communication~~

- Work with legal & forensics on who, what, when
- Assume threat actors are watching
- Know your audience
- Protect your IT team
- Document, document, document and debrief

Build Your Response Team

INTERNAL	EXTERNAL
• Technology • Communication • HR/Business • Superintendent • Risk Manager	• Legal Team • Forensic Team • Underwriters • Insurance Team

Know Your Policy

*Reimbursable Policy

1. Multi-factor for all remote systems access
2. Confirmation that firewalls/antivirus software are in place, and updated with critical patches within 30 days of release
3. Confirmation that employee cyber security awareness training has taken place in the last 12 months
4. Credible Endpoint Detection Response (EDR) tool is in place and active
5. Data backups are stored offline and require separate credentials to access that are maintained outside of Active Directory or stored in a cloud service designed to protect such data from a ransomware attack
6. Confirmation that network vulnerability scans regularly take place

District ADA Count	Member Retention (Deductible)
Compliant with Hamilton Six	Typically Lower Deductible
Non-Compliant with Hamilton Six	Typically Increase Deductible / or less coverage

Questions?

Shawnee **Nishimura**, Keenan
snishimura@keenan.com
(916) 640-6361

Jessica Blushi, Keenan
jblushi@keenan.com
(310) 212-3344

John Loyal, Cipriani & Werner
jloyal@c-wlaw.com
(610) 567-3576

Bill Hardin, Charles River Associates
bhardin@crai.com
(773) 415-3076

Kiley Heath, Mendocino County Office of Education
kheath@mcoe.us
(707) 467-5025

Thank you!

Complete Session Surveys on the PARMA App

Find the App, Click on Events, Click on Browse by Day, Click on the Specific Session, Click on Rate Event.