Cyber Incident Response 101

Stories, Tips and Tricks from the Front Lines

Topic

Using Ransomware as a framework, presenters will discuss current cyber events, the incident response process and some tools, tips and tricks to be better prepared.

Learning objectives

Attendees should take away a list of questions for their IT team, recommendations on tools and capabilities, and a checklist of incident response preparedness steps

"He's never hit an underground line in twenty years. He can wear anything he wants."

Introductions

Michael White

Partner

Carr, Riggs & Ingram

Will Daugherty

Chair, Cybersecurity

Norton Rose Fulbright

Serge Jorgensen

CTO, Founding Partner

Sylint Group

Agenda

- Who are the attackers
- What are they after
- Why do you care
- What can you do

Who are the Threat Actors

- Organized
- Professional
- Well Equipped
- Experienced
- Highly Motivated

What are they after?

By Victim Loss			
Crime Type	**Loss**	**Crime Type**	**Loss**
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

All of your files are currently encrypted by CONTI ransomware.
If you try to use any additional recovery software - the files might be damaged or lost.

To make sure that we **REALLY CAN** recover data - we offer you to decrypt samples.
You can contact us for further instructions through:
Our website
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://contirecj4hbzmyzuydyzrvm2c65aivslbuanj2cvf25zqj2dwrrqcq5oad.onion/

HTTPS VERSION:
https://contirecovery.best

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded your data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us ASAP

New Clients

Fuel Transport - 1% published
Tuckers Solicitors - 1% published
Outsource - 1% published
AppliChem GmbH - 1% published
Triad Mechanical Contractors - 1% published
The National Conference Center - 5% published
AMA Freight - 5% published
Holston Gases - 5% published
Parkway Products, LLC - 5% published
TRG Holdings, LLC

Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news!
P.S. We have the second domain: newsmaze.top.

To contact us use the feedback form of our news website.

Fuel Transport - 1% published

NEW

https://fueltransport.ca/

Article about Fuel Transport have been locked

Cryptoransomware

admin , 141

Read More >

Outsource - 1% published

NEW

https://outsource.net/

Article about Outsource have been locked

Cryptoransomware

Full dump

National Highways Authority of India - Full dump (100%)
LG ELECTRONICS - Full dump (100%)
Salini Costruttori S.p.A. - Full dump (100%)
Provincial Electricity Authority - Full dump (100%)
MaxLinear Inc. - Full dump (100%)
M.J. BRUNNER, Inc. - Full dump (100%)
Conduent, Inc. & Unamic - Full dump (100%)
Seats Inc. - Full dump (100%)
Critical Control Energy Services - Full dump (100%)
Optimara

From: John [redacted]
Sent time: [redacted] 2021 07:40:49 AM
To: Bill [redacted]
Cc: [redacted]
Subject: [redacted] rust Loan Payment Due $150,000 Reminder

Dear Bill:
I am writing to confirm our conversation of [redacted] 2021, that you should send payment of $150,000.00 from the sale of the [redacted] to [redacted] to the account of [redacted] attorneys for the [redacted] [redacted] Trust. The wire instructions are as follows:

Bank: SUNTRUST Bank, [redacted] 202

ABA No.: [redacted]

Account No.: [redacted]

Account Name: [redacted]
Special Account
[redacted]

If you would rather not do a wire, then you can send payment to the [redacted]

Please confirm when payment is sent either by wire or mail.
Very truly yours,
[redacted]

Business Email Compromise

- Access an account
- Find an invoice or email
- Send “updated” instructions
- Add rules to avoid detection

Why do you care

- Financial Loss
- Client Expectations
- Contractual Obligations
- Regulatory Requirements

Expectations, Obligations & Requirements

- Breach Notification Laws in the US: 50 states + DC and U.S. territories all have data breach notification laws the requirements of which vary from state to state.
- International Laws: For example, GDPR uses a much broader definition of "personal data" and requires to notice to DPA within 72-hours of breach
- Other laws
  - HIPAA: Requires HIPAA multi-factor risk assessment to rebut presumption of breach
  - Financial Institutions: Notice obligations may arise if the incident has a material impact on operations
  - SEC Reporting: Disclosure of "material events"
  - Defense Contractor/Sub-Contractors: DFARS requires notice to DOD (or prime-contractor for sub-contractors) within 72-hours of a "cyber incident" that affects a covered information systems or covered defense information
- Contracts: most contracts impose obligations to secure "confidential information" and to notify the other party "immediately" or "promptly" upon an actual or suspected breach
- Regulatory Landscape: regulators are increasingly aggressive, capable of diving into the technical details, and are not only interested in what happened in connection with an incident, but what the company was doing before the incident to ensure it had appropriate security measures.

What can you do

- Preparation
  - Tools
  - Testing
  - Assessment / Audit
- Response
  - Legal Counsel
  - Incident Response Team
  - Insurance

Legal Considerations

- How to engage a forensic firm to maximize privilege
- Ransomware - whether to pay the ransom
- Whether the incident is a notifiable event, who to notify, and when
- Engaging law enforcement
- Liability created by statements to employees and public
- Evaluating potential third-party liability and indemnification
- Cyber insurance coverage/exclusions

IT & Financial Controls Considerations

- How to engage with an auditor
- Identifying controls
- Assessing industry expectations
- Testing control implementation
- Balancing business vs. security

Security…

… or convenience?

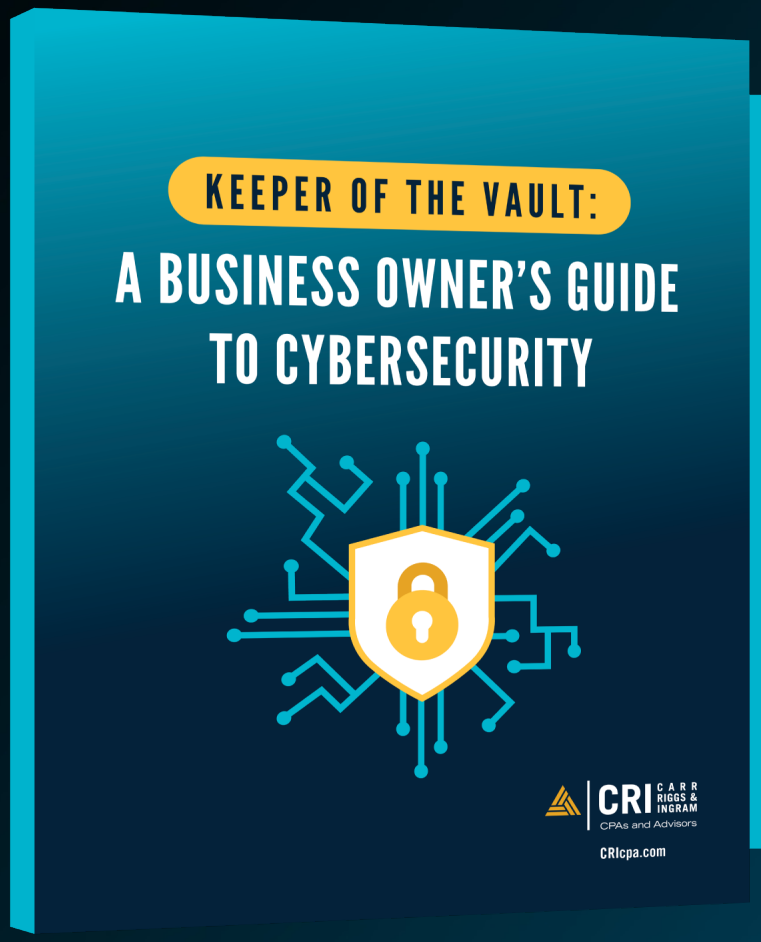
Preventative

- Multifactor Authentication (MFA)
- Endpoint Detection & Response (EDR)
- Immutable Backups
- Written Information Security Plan (WISP)
- Information Security Audit & Assessment

Responsive

- Incident Response Plan (IRP)
- Legal Counsel & Incident Response team
- Communications & Insurance Plans
- Tabletop Exercises

Takeaways



CRI E-Book:

Keeper of the Vault: A Business Owner's Guide to Cybersecurity

Michael White

mjwhite@cricpa.com

Will Daugherty

will.daugherty@nortonrosefulbright.com

Serge Jorgensen

sjorgensen@sylint.com