How to **severely lower** the risk of cyber crimes and **best practices** to being compliant

MAHU Meeting
June 16, 2022

1

TOP 20 CYBER INSURERS

2020 RANK	2019 RANK	GROUP NAME	DIRECT WRITTEN PREMIUM	LOSS RATIO W/DCC	MARKET SHARE
1	1	CHUBB LTD GRP	$404,144,104	41%	14.7%
2	2	AXA INS GRP	293,025,192	96.2%	10.6%
3	3	AMERICAN INTRNL GRP	228,424,711	100.6%	8.3%
4	4	ST PAUL TRAVELERS GRP	206,817,208	95.5%	7.5%
5	5	BEAZLEY GRP	177,746,192	47.9%	6.5%
6	6	AXIS CAPITAL GRP	133,549,784	46.2%	4.8%
7	7	CNA INS GRP	119,612,168	105.7%	
8	10	FAIRFAX FINANCIAL	108,687,558	55.7%	
9	11	HARTFORD FIRE 7 CAS GRP	102,864,503	25.4%	
10	8	BCS INS GRP	86,582,699	59.1%	
11	14	TOKIO MARINE HOLDINGS INC GRP	78,160,355	51.1%	
12	12	SOMPO GRP	72,588,641	114.1%	

U.S. Senate Unanimously Passes Cybersecurity Legislation Requiring 72 Hour Cyber Incident Notification

Thursday, March 17, 20

On March 2, 2022, the American Cybersecurity now with the House of R sent to President Biden's

Introduced by Senators the Bill uses language Reporting for Critical Information Security Mo Cloud Improvement and require critical infrastru

APRIL 8, 2022

State and local government agencies in North Carolina may not submit payments to -- or even communicate with -- someone who has encrypted their IT systems. Other states are considering similar legislation.

RANSOMWARE

North Carolina has become the first state to prohibit its agencies and local governments from paying ransomware.

ganizations legislation, state agencies and local submit payments to -- or even communicate crypted their IT systems. The legislation

FTC Chair Poised To Offer Glimpse Into Privacy Priorities

By Allison Grande (April 6, 2022, 10:47 PM

Khan prepares to deliver her first major

watchers are hoping she'll provide more

Insurance industry being ravaged by high rate of cyberattacks

By Brian Stone (Security N on April 8, 2022, 8:03 AM PDT

A new report from Black Kite shows the entire sector may be ripe for ransomware attacks.

It's time to make IT eas

How to severely lower the risk of cyber crimes and best practices to being compliant 2

2

Compliance Security Productivity

How to severely lower the risk of cyber crimes and best practices to being compliant 3

3

4

Agenda

- #1 Cyber Crime Today
- 5 Myths of Cyber Risks
- 3 Practices to Protect Against Crimes & Fines

5

Let's bridge the gaps

Daniel Metcalf
Managing Partner - CyberFin

- 15+ years of experience building technology solutions and services
- 5 years of experience providing cyber solutions for banks, credit unions and financial services organizations
- Responsible for bringing the technology and services together to protect your businesses

6

The #1 Cyber Crime Today

7

How to severely lower the risk of cyber crimes and best practices to being compliant 8

8

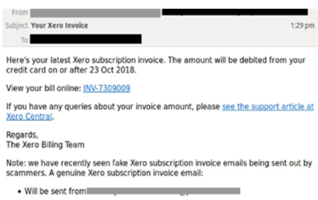
#1 Crime – The Execution

- Email Threats
- Malware infiltration
- Social Engineering
- DDoS
- Phishing
- Spyware

How to severely lower the risk of cyber crimes and best practices to being compliant 9

9

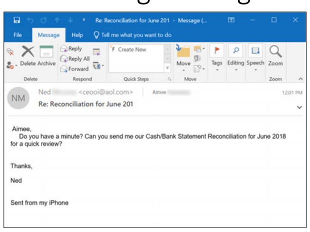
#1/2 Malicious E-mail Threat + Malware

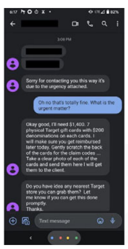


48% of malicious email attachments are Microsoft Office files

10

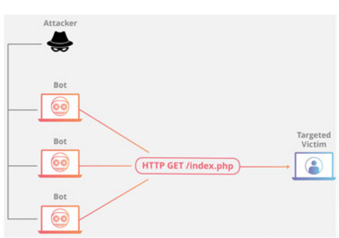
#3 Social Engineering





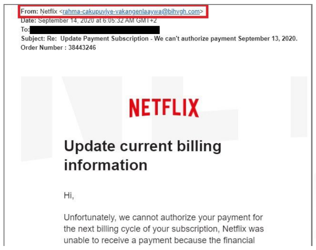
11

#4 DDoS



12

#5 Phishing


From: Netflix <rahma-cakupuvjye-vakangenlaaywa@bihvgh.com>
Date: September 14, 2020 at 6:05:32 AM GMT+2
To: [redacted]
Subject: Re: Update Payment Subscription - We can't authorize payment September 13, 2020.
Order Number : 38443246

NETFLIX

Update current billing information

Hi,

Unfortunately, we cannot authorize your payment for the next billing cycle of your subscription, Netflix was unable to receive a payment because the financial

How to severely lower the risk of cyber crimes and best practices to being compliant 13

13

#6 Spyware

Adware
Any software application that displays advertisements while the program is running.

E.g. banners, pop-up windows

Keyboard Loggers
A type of surveillance technology used to monitor and record keystrokes. Cyber-criminals can use these to steal sensitive information such as authorization credentials, enterprise data and computer activity.

Trojans
A software application that appears harmless but can inflict damage or data loss to a system.

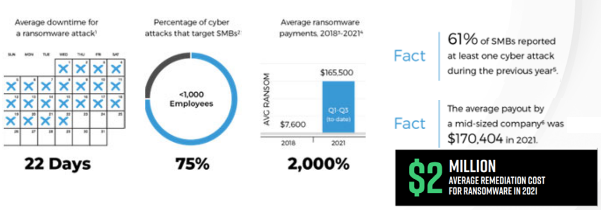
Mobile Spyware
A type of spyware that can infect mobile devices that typically enters via SMS or MMS communication channels.

TECHTARGET

How to severely lower the risk of cyber crimes and best practices to being compliant 14

14

Cybercrime – The Reality and Aftermath



[1]Coveware Marketplace Report (Q4 2020). [2]Covewareblog: Size of Companies Impacted by Ransomware in Q2 2021 (July 2021). [3]Corporate Compliance Insightsblog(June 2020) and 2020 Incident Response & Data Breach Report by Crypsis. [4]Stats found on www.coveware.com for Q1 2021($220,298), Q2 2021($136,576) and Q3 2021($139,739) indicate the average payment in Q1-Q3 was $165,53. [5]https://www.verizon.com/business/resources/reports/dbir/,6Sophos whitepaper: state of ransomware (2021)

How to severely lower the risk of cyber crimes and best practices to being compliant 15

15

The 5 Myths of Cyber Risk

16

Myth 1 – Size of agency matters

FACT – Small & medium-sized agencies are the *PRIME TARGET*

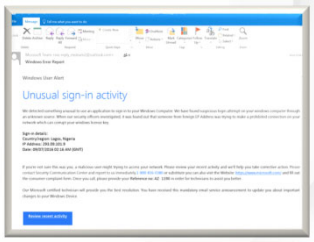
- Access to sensitive data
- Need to move the data to do business
- Run multiple attacks at once
- Lack robust security infrastructure
- "It's where the money is"

17

Scary Story – Bankrupt Agency

20 quotes to 25,000 in one month

- Received carrier site credentials
- Sold all data on dark web
- Remediation costs and fines bankrupt the agency



18

Myth 2 – The Cloud Protects Me

FACT – Cloud computing brings threat to the agencies that rely on it

- You are now the front door to data
- Cloud back up overwrites
- Cloud security and business-based app systems have severe gaps
- You become a mule

19

Myth 3 – The Homework is Easy

FACT – Clients do not necessarily want or need knowledge about cyber risk; what they really want is protection.

- Questionnaires, due diligence, audits, requirements… oh my…
- Few business/agency owners want to become Cyber Experts
- As bad guys get more sophisticated so does the information needed to protect yourself from each specific attack.

20

Myth 4 – Cybersecurity Risk Rating Tools are Best Indicators of Client Technology Risks

FACT – A glowing "cyber report" often leads to a false sense of security

- The best rating tools are rife with inaccurate results and false security
- Zero capability of predicting a problem or one's risk resiliency
- Does not include cloud computing or storage capabilities
- Simply does not tell you enough to make a judgement of cyber risk

21

Myth 5 – Choosing the Right Tools and Technology is the Best Place to Start

FACT – The technology and tools are only as powerful of who is managing it

- Alerts, updates, patches and remediation is an always-on activity
- Volume and sophistication are only increasing
- Fitting the tools for the management is more important than the technology itself

22

3 Best Practices to Severely Lowering Your Risk as an Agency

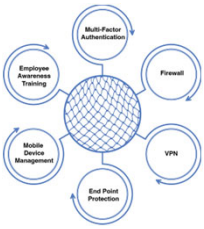
23

Auto Industry Example

Layered protection at the user level

24

Best Practice #1 – Mind the Gaps



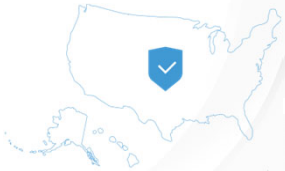
FACT – A layered security approach focusing on the end user severely lowers your risk profile.

25

Practice 2 – Ignorance is a Bad Defense

FACT – Follow the national guidelines

****Actively managing cyber security tools, policies and protocols keeps cyber-criminals, regulators, and underwriters out of your business



26

Practice 2 – Ignorance is a Bad Defense

A.C.T. Cyber Guide 3.0

Independent insurance agents and brokers must properly collect and protect sensitive client information every day.

CYBER GUIDE COMPLIANCE AND PROTECTION ROADMAP

1. Risk Assessment
2. Written Security Policy
3. Incident Response Plan
4. Staff Training & Monitoring
5. Penetration Testing & Vulnerability Assessment
6. Access Control Protocol
7. Written Security Policy For Third-Party Service Providers
8. Encryption of Non-Public Information
9. Designation of Chief Information Officer
10. Audit Trail
11. Implementing Multi-Factor Authentication
12. Procedure for Disposal of Non-Public Information

**ACT Guidelines

27

Practice 2 – Ignorance is a Bad Defense

NIST crosswalk to HIPPA

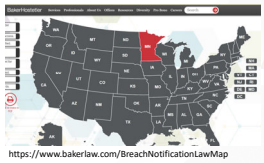
**Independent organization designed to create a national standard framework

28

Practice 2 – Ignorance is a Bad Defense

State Reporting – Definitions by state of:

- Personal information
- Persons covered
- Encryption / Notification Trigger
- Content requirements
- Timing
- Penalty
- Other Provisions



https://www.bakerlaw.com/BreachNotificationLawMap

29

Practice 3 – Look Less Attractive to Criminals

FACT – Criminals are lazy and are looking for R.O.I. Make your agency less attractive to crime.

30

Practice 3 – Look Less Attractive to Criminals

Create and require complex passwords with Multi-Factor Authentication

- 14+ characters
- Numbers, Upper and Lower Case
- Add Two Factor to e-mail, cloud and remote access

31

Practice 3 – Look Less Attractive to Criminals

Maintain separation of business and personal devices and activities

- Business only devices both in and out of office
- Home office extension of field office
- Business only e-mail boxes and log-ins
  - (eliminate @gmail, @yahoo, @live, @outlook)

32

Recap

- User-based layered security provides best protection
- Actively manage to one cyber security standard
- Authentication and complex passwords make your agency un-attractive to cybercriminals

33

Q&A

- Contact me directly for any additional questions
  - dm@cyberfin.net or
  - 612-888-0032

For more information visit us at www.cyberfin.net/TMA

34

Thank You

35