

Cyber Security/Trends in **Cyber Fraud and Cyber Insurance**



© Surry Insurance

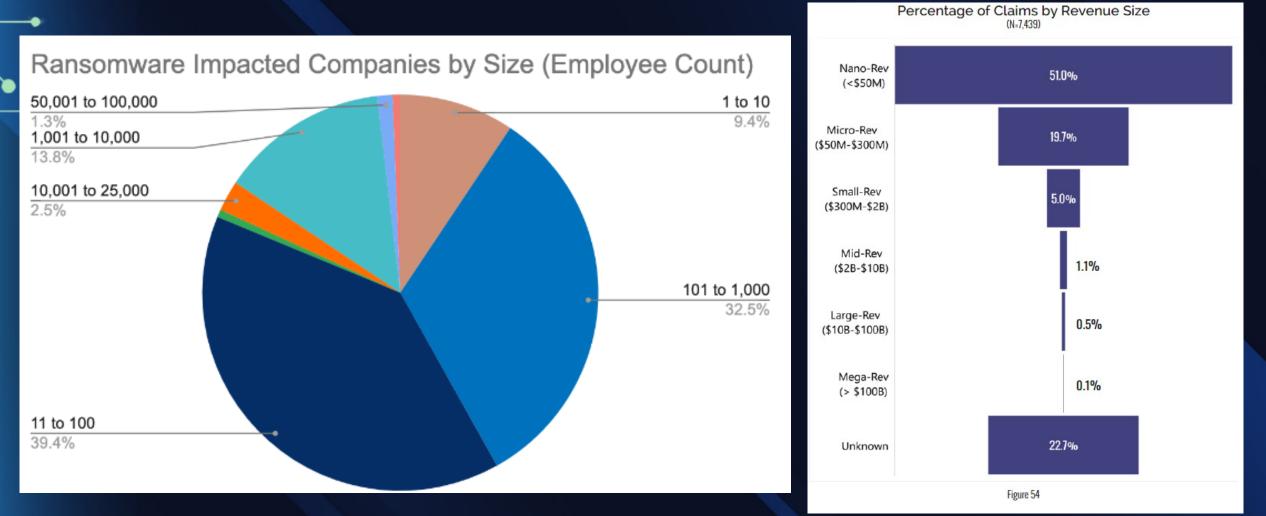
Local Government Facing Severe Level of Cybersecurity Risk

Cocal governments

- Health Care
- Schools

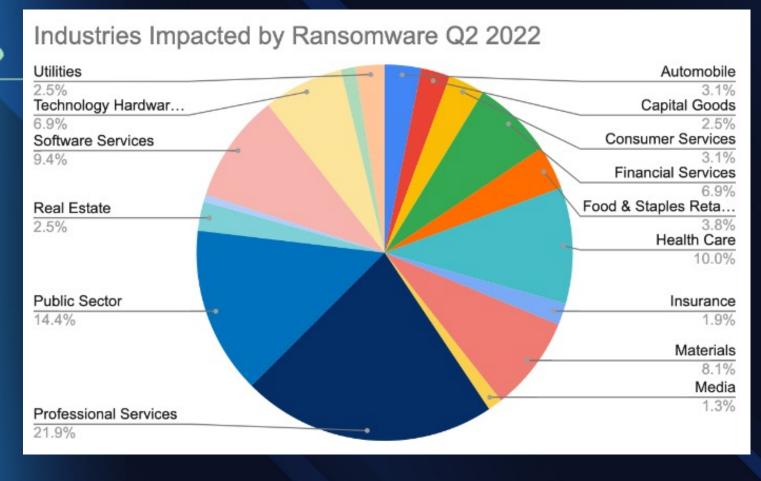
These three are particularly appealing "Soft Target"

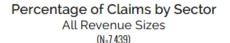
SIZE OF VICTIMS

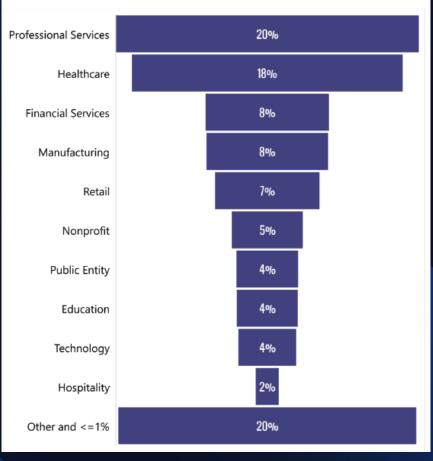


Q2 2022 Coveware

CLAIMS BY INDUSTRY







Data Breach Stories of 2018

Saks, Lord & Taylor: 5 Million records breached (April 2018) PumpUp: 6 million records breached (May 2018) Sacramento Bee: 19.5 million records breached (June 2018) **Tickfly: 27 million records breached (June 2018)** Panera: 37 million records breached (April 2018) Facebook: At least 87 million records breached (March 2018) MyHeritage: 92 million records breached (June 2018) Under Armour 150 million records breached (May 2018) **Exactis 340 million records breached (June 2018)** Aadhaar: 1.1 billion records breached (January 2018)

Source: https://blog.barkly.com/biggest-data-breaches-2018-so-f

Cyber Plan Action Items- Protecting Your Email

1. Set up a spam email filter

2. Train your employees in responsible email usage

3. Protect sensitive information sent via email

4. Set a sensible email retention policy

5. Develop an email usage policy

Source: FCC Small Biz Cyber Planning Guide

EMAI



Top 6 Causes of Data Breaches

- **1. Phishing (31%)**
- **2. Employee action or mistake** (24%)
- 3. External theft (17%)
- 4. Vendor (14%)
- 5. Internal theft (8%)

- **6. Lost or improper disposal of data** (6%)

Source: Is "Your Organization Compromises Ready" Baker Hostetler 2016 Data Securities Incident Response Report Property and Casualty 360 05/04/2016 article Your Data at Risk: 2015 Was a Year Full of Memorable Hacks by James Eng 12/13/2015

3 Ways to Safeguard Networks to Avoid Cyber Attacks

1. Establish a strong BYOD Policy

2. Protect local government-owned technology when it is offsite

3. Upgrade the way you send files

protect



Researching Cyber Risks

A recent study revealed that nearly onethird of U.S. local governments would be unable to tell if they were under attack in cyberspace and in some cases it was because of:

Lack of sound IT practices

Their IT policies and procedures were not in line with industry best practices

The Evolution of Network Security

Network security has evolved right alongside education technology. Departments can secure the data on their networks using many of the tools available today, such as:

Network Access Controls (NAC)

Antivirus and Antimalware Software

- Behavioral Analytics Tools
- Data Loss Prevention (DLP) Technologies
- Email Security
- Firewalls

) Surrv Insurance

- Virtual Private Networks (VPNs)
- Secure File Exchange Software



What Can Local Governments Do?

Choose network security tools with active scanning features. Go with tools that do most of the detective work for you.

Segregate your networks and hide admin SSIDs.

Use secure file exchange software that contains robust security features when sending and receiving files.

Lessons Learned

No Such thing as impenetrable IT systems

- Often times you do not know you've been hacked
- What is your response plan? Who is your 1st call?
- Encryption for sensitive data on portable media
- **Employee training matters**
- Monitor employee access to sensitive dataupgrade finance systems
- **Remote wipe capabilities**

Will soon ask for proof of insurance from vendors like you would ask for GL & WC

ESON



Hacking Terms You Need to Know

Botnets- Large networks of computers used by hackers to send spam and conduct widespread theft

- Denial of service-Used to interrupt a website/computer
- Internal Threats-Employees (both accidental & intentional)

Malware-Programs used by cyber thieves to hack networks

- Ransomware-Encrypts victim's data & demands money be paid to restore
- Social Engineering-Victims are tricked/deceived into releasing data or monetary funds

urce: propertycasualty360.com 12/09/201

Ransomware

UBMUFaOMO+Q+2nmU+4Pvhp33EE us2CE8nz9GBt+ab3Pbo9On2MMyGn1h]zTNyzIBOKburn wmOJ7LYVVQThyzBt61KDPExN6 Y+6NtXFqS901XNREf3kIjn. ZLdr2sOM5WZXGp7j05EFFFqisV ZolltHHjFn1SBPUgoF/3GhmMy kOwx2sqA+SGbYLj9KAFveev5vD/PR zeCzhuTc+N7vkxi/pkmUA5YtBeh E3NPWXT0V9 13ilkrjUe2Aj5ZiacGpRAp14KEhFRHf1 wgYJ1Y30axSC DHMPFsQ9b4AtTfIbgZtu1QGjfTVOq 8FuaWqegyYLtSSD18PYKVtSWBFZ+1IZ0p oD7wbga4ndvp wDftdtG5yGMHbMdZRz/hyv0IAprhi6s Lj4gcOeOdaKwwl0cp40uSed7IGV/y6Pzhqw uc2vBvG/JzpQk thFc5i2zHpbFcGWTpTtwqF0v7jAHMmj2y u2yyxC79YaasImkxc9XSelu63G3Kx0k3m08d hhEQf4rM9TDLvL eM2T2NtB15Hvnk8ThZ4OZ7F6Crnghtqzk0 lSmgX1/BEeRB4PkBG6fSufCOK/wgcDHexCu GyDsCzrpDGFEiMeGcXtBWO+R0bqnup4f k4Pi86UzV3z67CY10DIDgxoFyA3awS7Tdvdv 6P3PFbUSrflGCcxel0jKMfYncAAzqDh0rl Ir0yqv2/uRVgMXg41Xi5Tc4xDdAza+45Nw34P ubb vaD06xU2N8m8jWYA/03hD8iKaIQjT+y43q yg9WmuDfg00HLhT4Gwj/6qLe0ofc1khjY6756 MCTL GXYQh31cB04n1Cy4Ua3D3UJjsGe5U/YozY aVPZT/Z6Wow/G8I1aaK003Rgo8tL+HgyIHNCR XPZ) zSGsV9ZpHi/h/eMNFlJxamtM6y/iZOX3d49 Mpmi+pLq0pC9gJJg38H6PuUZS0UOX1TGbeLnx zrvj +WiplgRT3SuVlzz6rgC47pD6M3GvG4vCmOM 4itLIx009JevudvwLoLUjZ0VzGro8UfN9G3Av7 it5 eGykkHnt2wuqfQd9FJJmgynvpsRiB3Su4Ez D8BkuBqEB1Qv0qKv0tfjHa0078KovcDkzbEDY sXX5xc7mhqOBStc0B7aE29KOgtvrf/iRuIL RXMPcFcgnaqGg1ZBsJbZTG+qoCKDo3Nj1Izmr Fs6silRnzh19Fd1f6SdNZSH+Nw8xCL9j4p VCdg4UuLEawlvXLaZe24FAEdbpDNgJT4BgtOArcVxHUOSTtU1gsARgUd0Zmyf5a9YnByQGTI6rrICRiAFZj1+teNJiA2T TdOUyHx13Ks/tCyIA6BBMW6Nvg/VLKnfFzyCPdkZfRLa7WUjVggXhASRXys7xR9677Mp37+nEaFdbrwvIiN9hhG6HS1 HpP2GhLf8F -- ' ' vVkx7NZ HmK7+ftt

> 6xyygF4xiYjlgxkMCUyQZ9/d5ehMUPLo4c4hIXAXuKHfUUHVt* PAK2pCeQo4c8VpdtZNegdUaYPT3LtNJm17kAaf ARAUVSTEETE IN

uu101010101010101010101010 useseseseseseseseseses u\$956565959595050595959595954 ************************* ·1010101010101010101010101010 -##### 10 6 10 565u **U668** 1154 \$\$\$1 **** 0555 *\$\$\$\$\$uut08 \$05uut565* ********* ******* u0001000000000000000 48-8-8-8-8-8-84 stut 6 6 6 tutt 101070 6640a9u848466 u5555 u5555 +19191959595+ ******* \$\$\$\$\$**\$**ua ----- uuus96868686868 10000000000000 warau **555555555559auta #866uuef6666666664m ++56666666666666666 ******** **************** *\$\$555 ******** 000-PRESS ANY EXT. 0208*

matificalie.c.t.

noyN93

TYS5

15

How Does a Ransomware Infection Occur

A typical ransomware infection can begin with any of the following routes:

Email messages that carry a downloader Trojan virus, which attempts to install ransomware

Websites hosting exploit kits, which attempt to exploit vulnerabilities in the browser and other software to install ransomware

How Do I Protect My Computer Against Ransomware?

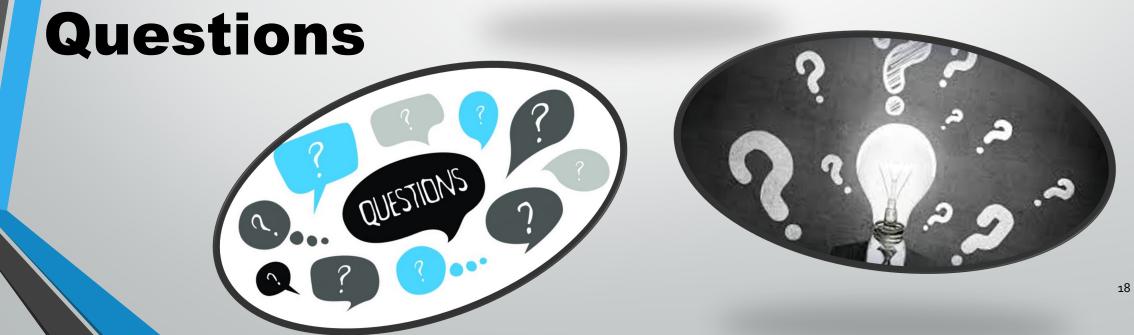
Regularly back up your important files. Consider using the 3-2-1 rule: Make 3 backup copies, store in at least 2 locations, with at least one offline copy. Use a cloud storage service.

Install and use an up-to-date antivirus solution

Don't open emails/attachments from unknown sources

Make sure your software is up-to-date to avoid exploits





Money and Securities Coverage



© Surry Insurance

The Basics- Money and Securities Coverage Form

- Provides coverage for money and securities in the event of theft, disappearance, or destruction caused by a third party.
- Coverage is provided while inside your premises or inside a bank premises.
- Coverage is provided while the money or securities are in the care of a messenger outside your premises or the bank premises.
- Limited coverage is available for damage to the premises including the safe or vault during an actual or attempted theft.

Questions

Plain and simple, what kind of criminal act(s) are we covering with this policy?
We know who third parties are by now, but who are messengers?



Claims Scenarios

Non-employees (robbers and burglars) break into a property seeking cash and other items such as computers and laptops. The cash would be covered under Money & Securities coverage, and the computers and laptops would be covered under the property policy.

Where does your departments have the most cash exposed to theft by others?

Other examples?



Worth noting, you could have two deductibles



22

Computer and Funds Transfer Fraud Coverage

A Computer Fraud policy provides coverage for theft of money, securities, and property (inventory) involving the use of a computer that would fraudulently transfer money, securities, or inventory from inside your premises or inside a banking premises to a place outside of these locations.

Computer and Funds Transfer Fraud Coverage

- Funds Transfer Fraud coverage would cover the loss of money or securities after an electronic, telegraphic, cable, written, or telephone instruction that was fraudulently transmitted to a financial institution instructing the financial institution to release money from your account to a third party's account.
- These are third party claims. If employees were doing this, if would be an employee dishonesty claim.

Questions

What is the difference between the two coverages?

Computer Fraud is the use of a computer (hacking viruses, etc.) to cause of transfer of cash or inventory.

Funds transfer fraud results from a fraudulent communication (email, fax, etc.) directing to a financial institution to move cash or securities to another account.

25

cyber

Shif

Claim Examples

Viruses online and contained in emails

- Email addresses captured and used for attempted funds transfer
- Lost or stolen laptops and/or zip drives with account information used to attempt transfers





Fraudulent Impersonation Coverage



© Surry Insurance

Fraudulent Impersonation Coverage

 This is the latest Commercial Crime Insurance coverage available
Offered in response to a new twist on an old crime

Fraudulent Impersonation Coverage

In Property Insurance terms, this is a "voluntary parting" under a standard commercial policy.

- If it is damaged by fire, lightning, wind, hail, etc. the property is covered/
- If property is stolen by criminals (computers, laptops, lawn mowers, tractors, etc.

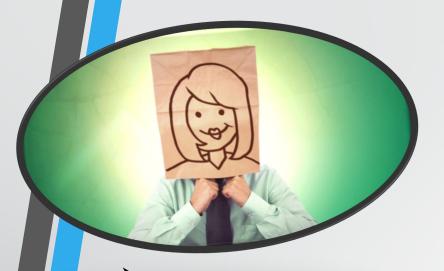
Problem occurs when you willingly give the property to a thief

Voluntary Parting is expensive coverage and is usually provided as a sub-limit

Fraudulent Impersonation Coverage

Now the "twist" is where do we get coverage when we actually give the money away due to a fraudulent scheme?

Enter- Fraudulent Impersonation Coverage (Form CR 04 17)



The Basics

The policy will provide coverage under <u>two</u> scenarios:

Fraudulent Impersonation of Employees

Fraudulent Impersonation of Customers and Vendors

Fraudulent Impersonation of Employees

The school makes a good faith transfer of money, securities, or other property in reliance upon transfer instruction purportedly issued by an employee or any of your officials if under a Government Crime Form.

Scenario of a Customer/Vendor Claim

Criminals impersonate an IT vendor and emails an invoice for work they say was completed (or not?) and want the money sent to them (the imposter)

Actual claims or close calls?

Would any of you care to discuss an actual claim or very close call?

Questions



If you would like a copy of this presentation please email derek.slate@surryinsurance.com