



Cyber Security/Trends in Cyber Fraud and Cyber Insurance



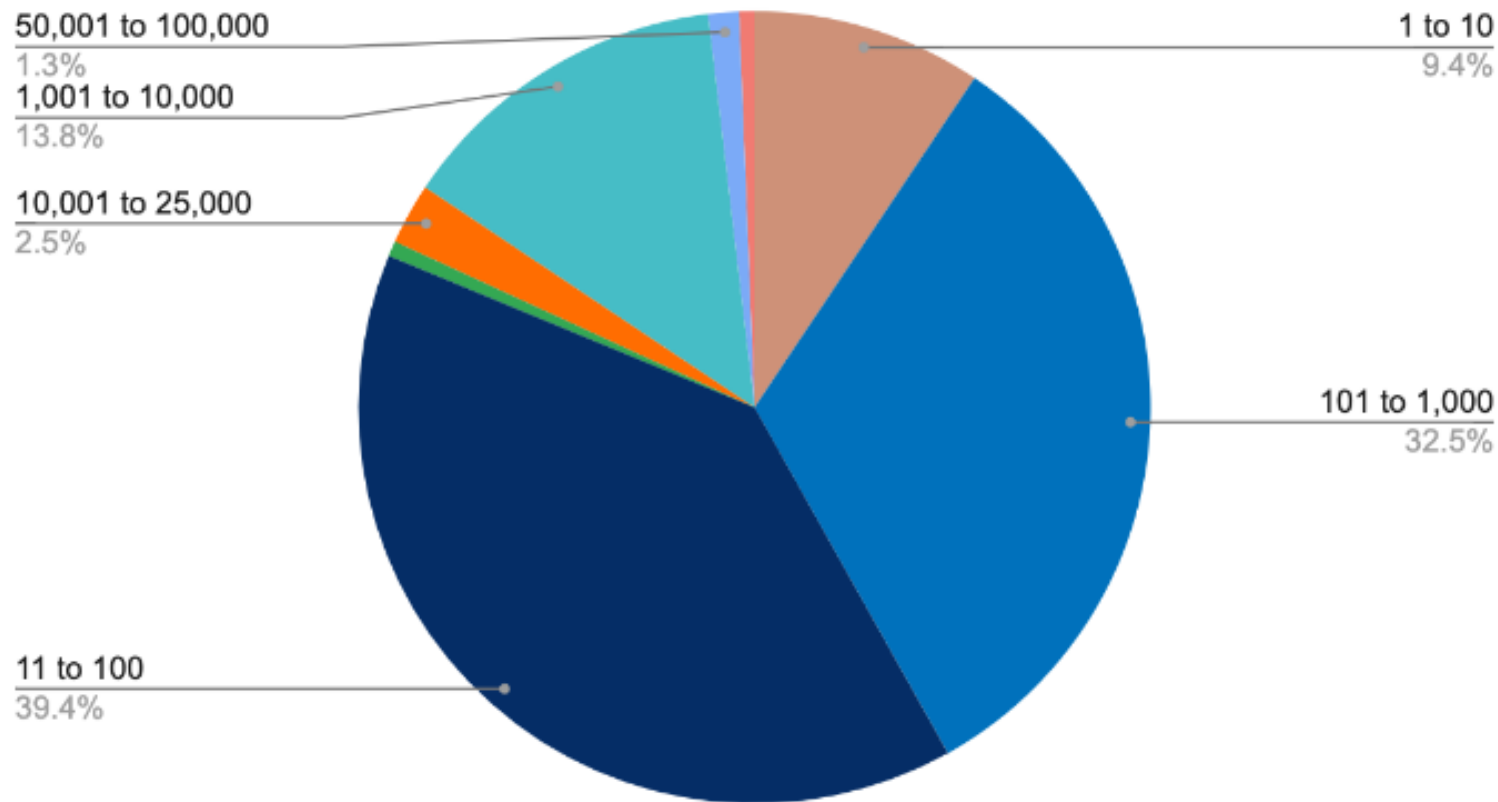
Local Government Facing Severe Level of Cybersecurity Risk



- **Local governments**
- **Health Care**
- **Schools**
- **These three are particularly appealing “Soft Target”**

SIZE OF VICTIMS

Ransomware Impacted Companies by Size (Employee Count)



Percentage of Claims by Revenue Size (N=7,439)

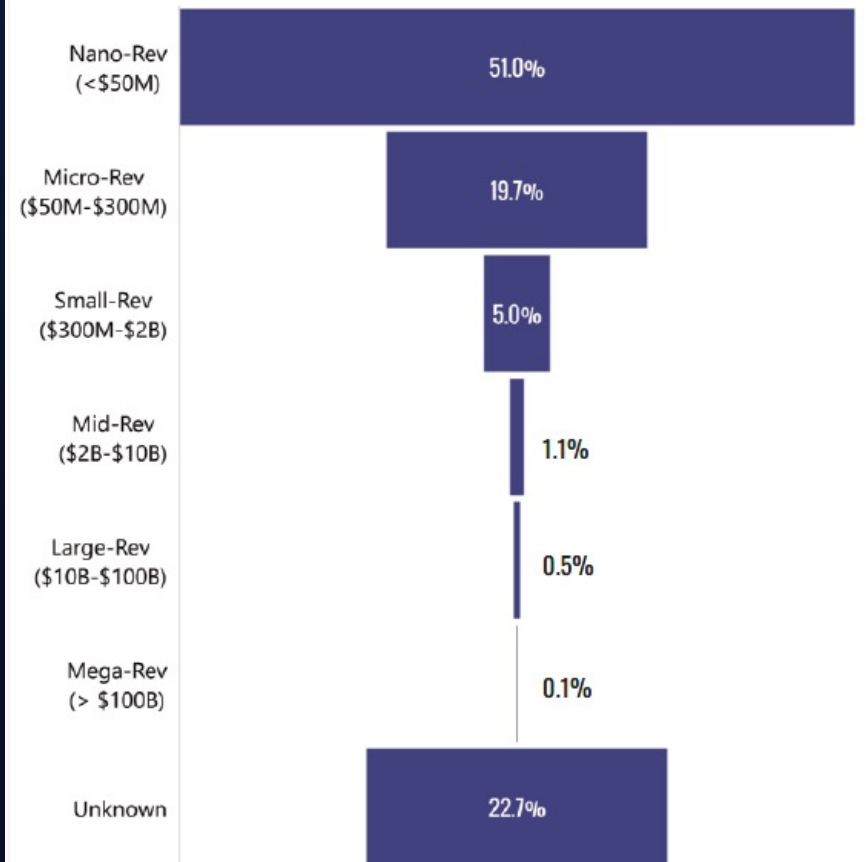
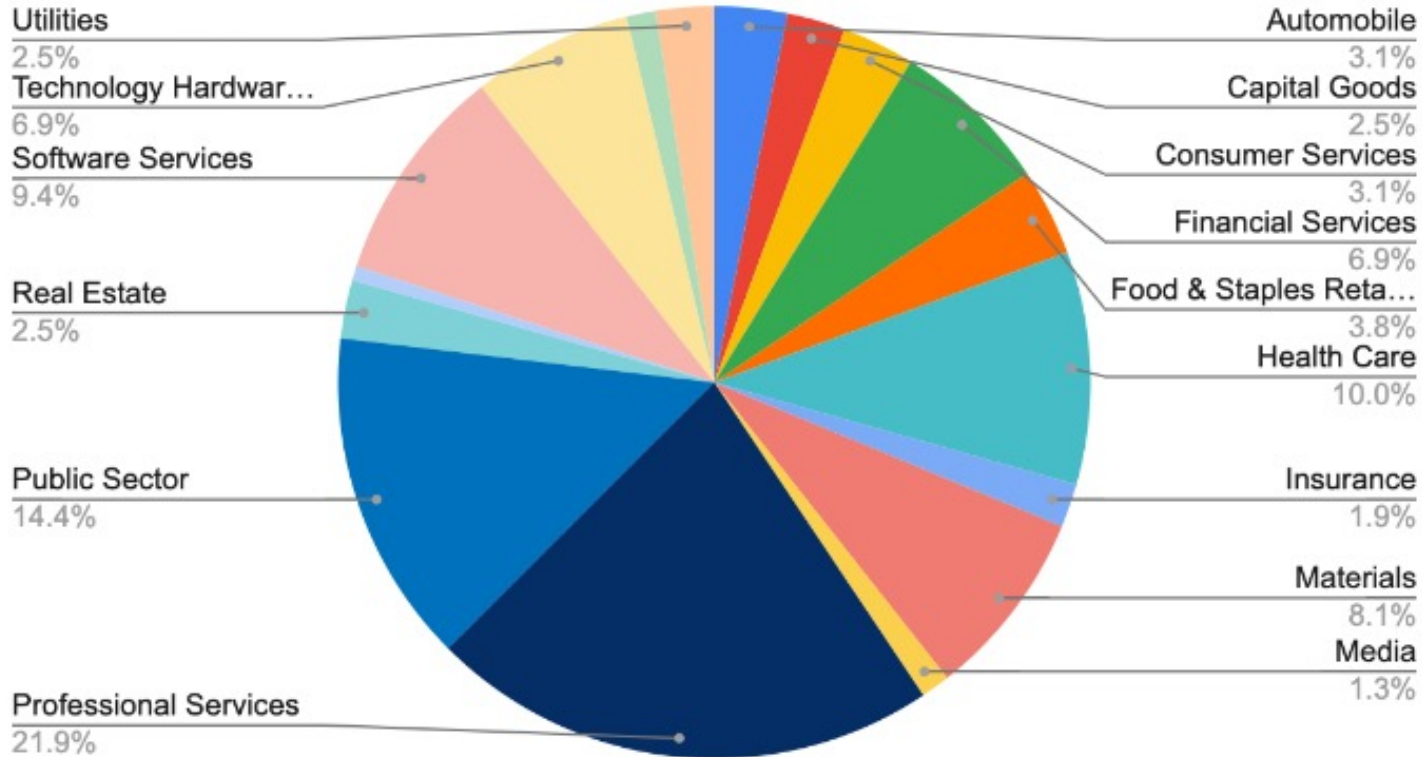


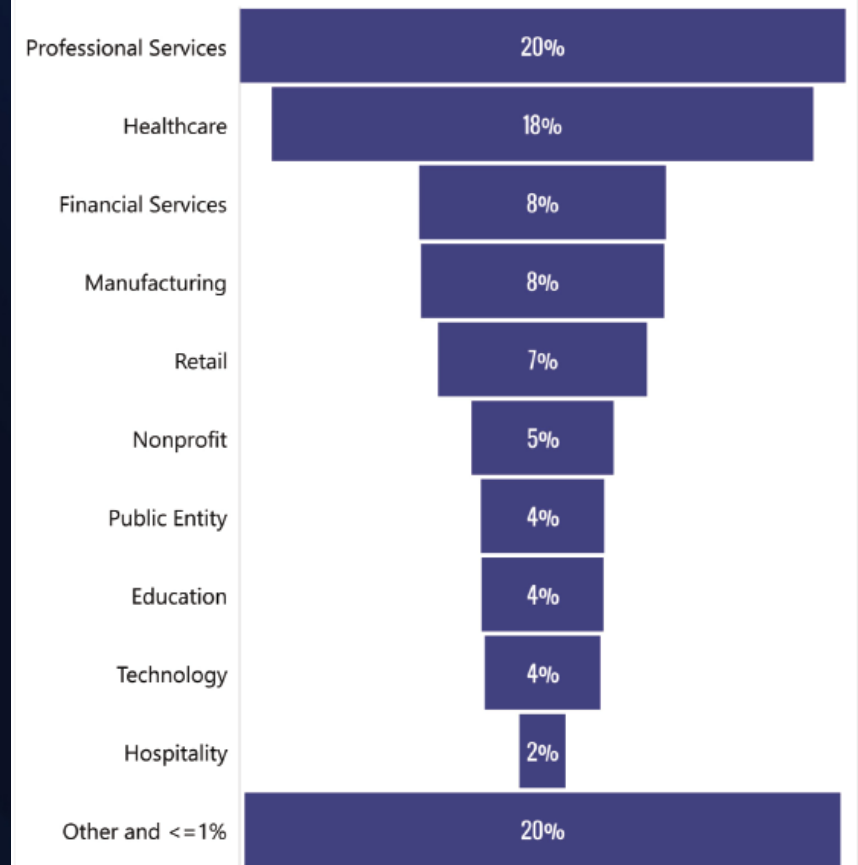
Figure 54

CLAIMS BY INDUSTRY

Industries Impacted by Ransomware Q2 2022



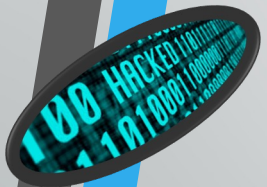
Percentage of Claims by Sector
All Revenue Sizes
(N=7,439)



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-far>



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

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%)**



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**



➤ Source: <https://www.xmedius.com/en/blog/3-ways-safeguard-school-networks-avoid-cyber-attacks-infographic/>



Researching Cyber Risks

A recent study revealed that nearly one-third 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**
- **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 data-
upgrade finance systems**
- **Remote wipe capabilities**
- **Will soon ask for proof of insurance from vendors
like you would ask for GL & WC**



CARTOONSTOCK
.com
WILDT
Search ID: cwln8506

· "No, I'm not writing a short story.
That's my password."

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

Source: propertycasualty360.com 12/09/2015

Ransomware




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**

Questions





Money and Securities Coverage





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.**

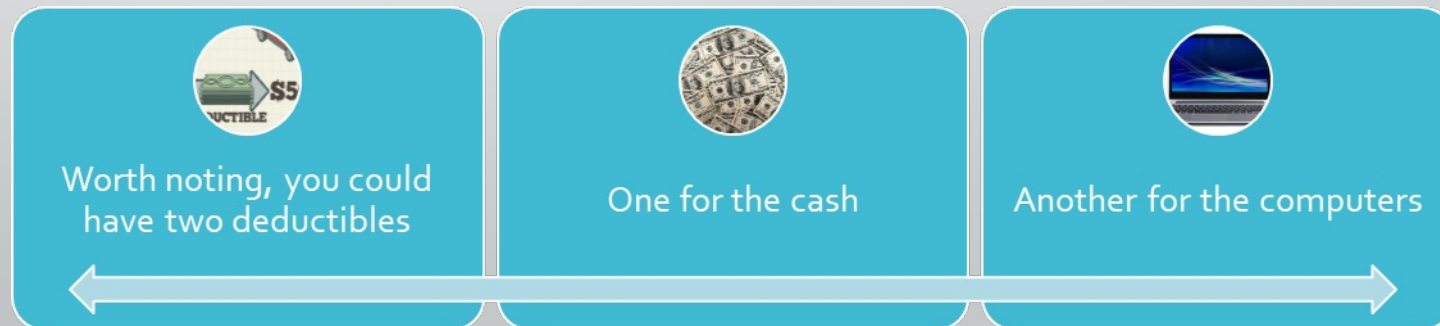
Questions

- **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?**



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, it 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.**



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



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 two 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**