APCO International
Leaders in Public Safety Communications®

Cybersecurity Committee

Cyber Insurance Whitepaper for Public Safety Agencies

June 2024

Cybersecurity Insurance and Emergency Communications Centers

Introduction

Cybersecurity insurance is an option that many public safety agencies should consider. This whitepaper is intended to provide information on why you may need it, what it is, and the factors that affect its cost and availability.

The Threat

The threat of cyberattacks on public safety emergency response capabilities has grown significantly in recent years and the upward trend is expected to continue. Emergency Communication Centers (ECCs) can come under attack[1] for a variety of reasons that range from collateral damage, not being the intended target, to deliberate attempts at emergency services interruption.

The main drivers of increased risk are a combination of decreasing costs to launch attacks coupled with the ability to derive economic gains from the attacks. In short, the cost/benefit equation is attractive to cybercriminals[2]. That equation varies by target. Jurisdictions that invest in cyber defenses and adopt policies that reduce the chances of a successful attack are less likely to be targeted by cybercriminals. Unsurprisingly, cyber insurance is less expensive and more available to those jurisdictions that actively reduce their risk.

Two of the most common cyberattacks affecting ECCs are ransomware and denial of service (DoS). Both compromise the ability to function and have the risk of full impairment. Email phishing is related to ransomware in that it can serve as the method of breach. Operational impacts can range from the loss of critical systems, like call taking workstations or CAD, to the need to alternate route calls for extended periods of time[3].

Mitigation Strategies

There are several actions which you can take to protect your agency from cyberattacks. The APCO Cybersecurity Committee has created a guide that will provide a good starting point with[4]: An-Introduction-to-Cybersecurity-A-Guide-For-PSAPs-1638566090.pdf (911.gov) .

© 2023 APCO International

At a high level, recommendations can be divided into three categories: prevention, detection, and reaction.

Prevention

The foundation of prevention is awareness. Knowing that you could be attacked and altering behaviors and policies to reduce risk is the starting point for cyberdefense. Although not always easy to implement, preventative measures are often low cost and have a high impact. The ability to demonstrate that your organization has adopted best practices designed to thwart cybercriminals is also an excellent way to get cybersecurity insurance at the lowest available rates.

Detection

Tools for detection of cyberattacks, especially those that are focused on a specific target, can be prohibitively expensive. Keeping up with the technological arms race between attackers and defenders requires regular investments and disciplined attention to current events. For public safety agencies, the best option is often a service(s) provided by their existing vendors. Cybersecurity monitoring services can achieve economies of scale that lower unit costs and provide access to scare subject matter experts on as needed basis[5].

Reaction

How you react and the speed with which you act are determining factors in the amount of damage you sustain from a cyberattack. Experience has shown that creating and maintaining a cyberattack response plan can make a major difference in the outcome. An agency that is well prepared and has pre-planned actions is in a much better position to respond to a cyberattack. The ability to recover quickly in the aftermath of an attack is significantly enhanced through cyber insurance. Policies can make resources available on an accelerated timeline and often include access to subject matter experts.

Cybersecurity Insurance Attestation

Attestation is required before companies offering cybersecurity insurance will quote available options and pricing. Simply put, it is one or more questionnaires that seek to document your current cybersecurity practices, defenses, and risks[6]. Any quotes you receive will use your answers as the basis for pricing and availability. If you decide to purchase cybersecurity insurance, payments will only be made if the insurance company confirms that you met the attested pre-conditions. In some cases, the insurance companies will seek to verify your answers before the coverage goes into effect, but the risk of non-compliance stays with your agency in either case.

This practice, common to all types of insurance, provides a useful checklist of steps you can take to lower risk. By reducing the risk taken by the insurance company, you are also reducing your own risk. It is highly recommended that you utilize the best practices and technologies which are designed to lower risk, regardless of whether you decide to purchase cybersecurity insurance. The best insurance policy is often the one you never need to use.

© 2023 APCO International

Again, with or without cybersecurity insurance coverage, another important takeaway from this insurance industry practice is to have a cybersecurity plan and a disciplined approach to maintaining your defenses. This is true for policies as well as technologies.

Cybersecurity Insurance Coverage Options

As stated above, the role of cybersecurity insurance is to reduce the time to full recovery by providing a source of funds that are readily available. There are several options available[7]:

First-Party Cybersecurity Insurance Coverage

This type of insurance protects your agency from direct losses due to a data breach or attack including employee and customer information. Examples include:

- Fraud & Theft (Hacking activities)
- Forensic Work (Accounting costs)
- Business Interruptions (Deliberate denial of service and Lost income)
- Extortion & Blackmail (Negotiation & payment of ransomware demand)
- Loss of Data & Restorative Work (Data destruction and recovery & replacement costs)

Third-Party Cybersecurity Insurance Coverage

This type of insurance protects your agency from liability when a citizen, partner, vendor, or other party sues following a breach. Examples include:

- Litigation Coverage (Legal fees) (Settlements)
- Regulatory Coverage (Fees, fines, and penalties related to the incident)
- Communications & Notifications (Breach notification to customers or setting up a call center)
- Crisis Measures & Emergencies
- Credit Monitoring & Review (Identity restoration)
- Liability for Media Issues (Recovery of intellectual property)
- Liability for Breach of Privacy & Confidence (Errors & omissions)

What Cybersecurity insurance Usually Will NOT Cover

- Bodily Injury or Property Damage
- Loss of Property
- Intentional Acts (Intentional, dishonest, or criminal acts by the agency)
- Weak Security Posture (Minimum steps not taken by the agency to protect themselves)
    - Email Security
    - Identity/Access Permissions
    - Multifactor Authentication Use
    - Data Encryption
    - Backups

© 2023 APCO International

- Security Awareness Training
- Network Security
- Compliance Frameworks & Standards Adherence
- Response Plans

Take note of the exclusion of coverage and often complete unavailability if you have not taken basic steps to prevent an attack. Prevention is the best defense.

Pros and Cons of Cybersecurity Insurance

Pros[8]

- Establishes coverage for legal and financial support in the event of an incident.
- Gives insured party access to forensic and or restoration resources.
- Provides a baseline cyber framework posture or allows insured to inquire about how to decrease threat vectors.
- Fulfills possible regulatory requirements.
- Assists agency with customer notifications, if needed in the event of an incident and helps restore personal identities of affected customers/users.
- Allows agency internal staff to begin organization-based cybersecurity program and set internal guidelines or policy.
- Coverage could include lost/stolen devices, data corruption/theft, crisis management.
- Risk mitigation
- Support services included with policies.

Cons[8]

- May require business impacting restrictions-based policy coverage specifications, or insurer may dictate specific remediation steps.
- Inconsistent pricing from insurers, agency will need to know levels of detail on their internal protection levels or be able to price out a risk strategy.
- May not cover loss of intellectual property or public relations fallout from an incident.
- Does not replace the need for cyber defense or an agency-based cybersecurity program and response planning.
- Debate by some professionals on if cyber insurance creates a market for cybercrime and ransomware attacks.
- Generally, does not cover the following – poor security processes, prior breaches, human error, insider attacks, pre-existing vulnerabilities, needed technology system improvements, infrastructure failures, or physical damage.
- Costs
- Limited availability

Funding Sources

© 2023 APCO International

Enhanced cybersecurity has benefits that go beyond your agency's boundaries. A strong cyberdefense posture is in our national interest and we are all better off with widespread adoption of best practices, which can include cybersecurity insurance. The collective benefit is reflected in the increasing availability of funds from federal, state, and local sources for improving cybersecurity.

APCO International advocates for more funding as part of our commitment to public safety. It is strongly recommended that you monitor grant availability and apply for those that fit your needs.

Conclusions

Each ECC needs to make its own decision based on circumstances and available resources. All ECCs should carefully consider cybersecurity insurance options when reviewing their cybersecurity risks and plans. The best available policies at the lowest costs can be found when your agency adopts good cybersecurity practices. Insurance is most helpful after a cyberattack. Having rapid access to funds and expertise can accelerate recovery and limit damage.

References

1. *Cyber Incident Response to Public Safety Answering Points: A State's Perspective* https://www.cisa.gov/sites/default/files/publications/22_0414_cyber_incident_case_studies_state_final_508c.pdf
2. *CYBER INSURANCE: Action Needed to Assess Potential Federal Response to Catastrophic Attacks* GAO-22-104256, CYBER INSURANCE: Action Needed to Assess Potential Federal Response to Catastrophic Attacks
3. *Why Every PSAP Needs to Be Vigilant About Cybersecurity* https://urgentcomm.com/2018/11/02/why-every-psap-needs-to-be-vigilant-about-cybersecurity/
4. *An Introduction to Cybersecurity: A Guide for PSAPs* An-Introduction-to-Cybersecurity-A-Guide-For-PSAPs-1638566090.pdf (911.gov)
5. *Creating a Culture of Cybersecurity in America's 911 Call Centers* Creating a Culture of Cybersecurity in America's 911 Call Centers | Federal Communications Commission (fcc.gov)
6. *The Pros and Cons of Cybersecurity Insurance for Municipalities* Pros & Cons of Cyber Insurance for Municipalities | StateTech Magazine
7. *Types of Cyber Insurance* Types of Cyber Insurance - CyberInsureOne
8. *Cyber Insurance Explained: Costs, Benefits, Coverage & More* Cyber Insurance Explained: Cost, Benefits, Coverage & More | StrongDM
9. *Cyber Insurance (Small Business Guidance)* https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance
10. *What is Cyber Insurance and Why is it Important: Definition* What is Cyber Insurance and Why is it Important? | Definition from TechTarget
11. *Five Types of Cyber Insurance and What to Watch Out For* 5 Types of Cyber Insurance Coverage and What to Watch Out For (bluevoyant.com)

© 2023 APCO International

12. *Cyber Insurance 101: Understanding the Basics of Cyber Liability Insurance* Cyber 101 Understand the Basics of Cyber Liability Insurance | Woodruff Sawyer

© 2023 APCO International