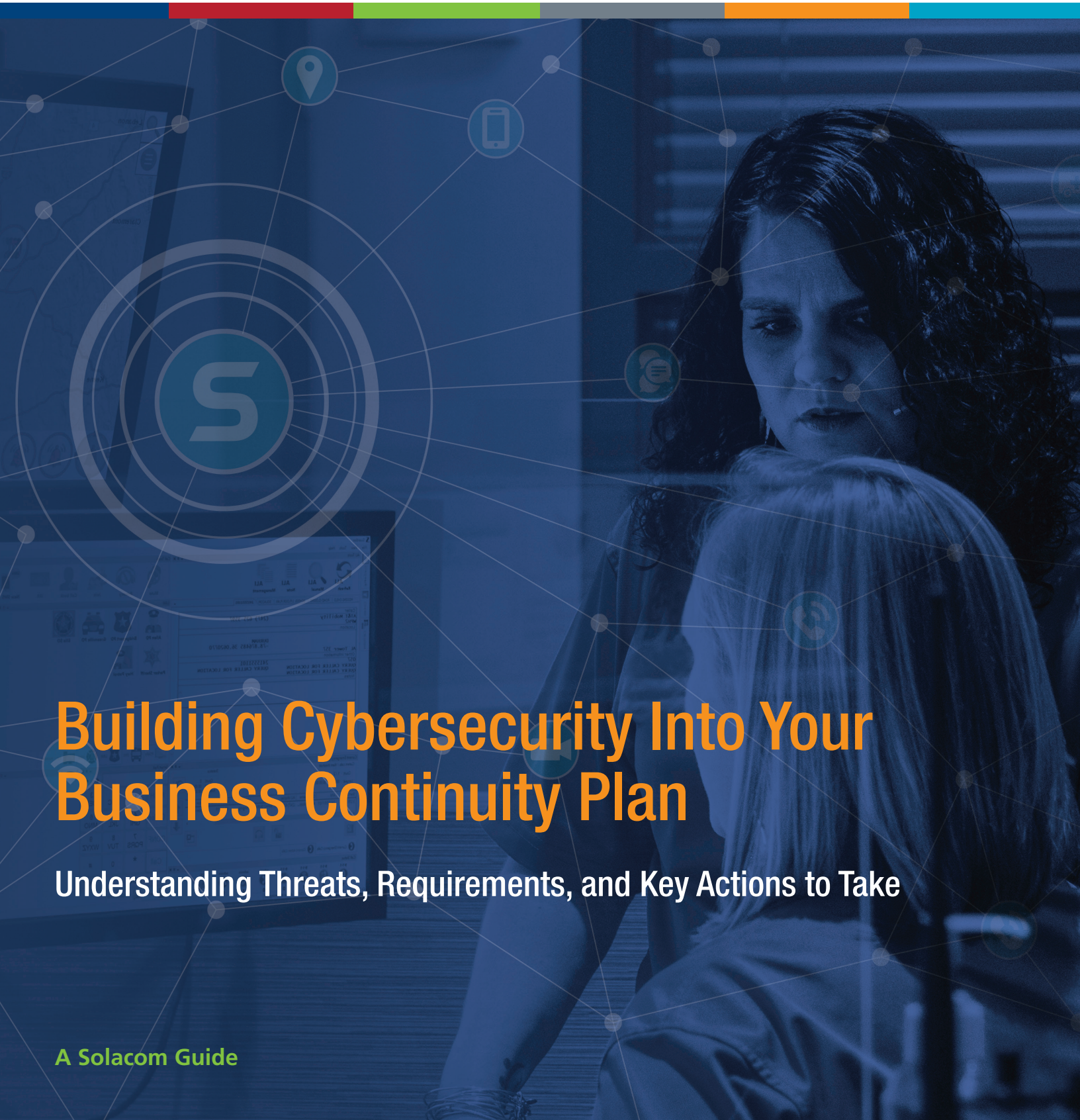
SOLACOM



Building Cybersecurity Into Your Business Continuity Plan

Understanding Threats, Requirements, and Key Actions to Take

A Solacom Guide

Every public safety answering point (PSAP) already has a business continuity plan that describes contingencies and processes to follow should a man-made or natural disaster affect PSAP operations. From situations involving fires and floods to gas leaks, building system failures, and bomb threats, PSAPs have detailed plans in place to help ensure personnel remain safe and the public continues to have access to 9-1-1 services.

As PSAPs evolve toward Next Generation 9-1-1 (NG9-1-1) call handling and management systems, it's more important than ever to build cybersecurity measures into their business continuity plans.

Cybersecurity Threats Are Evolving

With the move to IP-based NG9-1-1 systems, new cybersecurity threats that can hamper or halt PSAP operations have emerged. At the same time, there's been an increase in the numbers, types, and sophistication level of cyberattacks around the world.

Today, most PSAPs are aware that cyberattacks pose a serious threat to their operations. And they know that cyberattacks are on the rise. But, PSAPs are not always aware of the cyberthreats that are most likely to affect their operations and what can be done to help mitigate the risks associated with cyberattacks.

To effectively build cybersecurity into business continuity plans, PSAPs must ensure they understand the:

- Full scope of cybersecurity threats and risks in NG9-1-1 environments
- Strategies and solutions needed to mitigate cybersecurity risks and threats
- Key actions they should take when building cybersecurity into business continuity plans
- Role that NG9-1-1 cybersecurity experts play in mitigating cybersecurity risks and helping PSAPs ensure business continuity

To help PSAPs increase their understanding of cybersecurity in NG9-1-1 environments, this guide outlines three steps every PSAP should take to build cybersecurity into a business continuity plan.

STEP 1

Prepare for a Range of Potential Cyberattacks

Understanding the full breadth of the threat and risk landscape in NG9-1-1 environments helps to ensure the appropriate cybersecurity mitigation and containment measures are put in place.

Cyberthreats and risks to PSAP operations can be grouped into three main categories:

- Network infrastructure and connections
- Users and devices
- PSAP services

Network Infrastructure and Connection Threats

The network is the doorway to all of your systems. Once hackers gain access to the network infrastructure, they can potentially access every computer and system that is directly and indirectly connected to the network. This vulnerability is a key reason that PSAPs must have strong and open communications with their network and internet service providers. We'll talk more about that aspect of cybersecurity in the next section.

Unauthorized network access can also be used to launch denial-of-service (DoS) attacks that overload network resources with requests for access. DoS attacks can cripple the network so it is extremely slow or overwhelm it completely so it is unable to process valid requests from PSAP systems.

Because PSAPs rely so heavily on telephony to provide 9-1-1 services, telephony denial-of-service (TDoS) attacks are a particularly important threat to understand. A TDoS attack uses Voice over IP (VoIP) systems to overload phone systems with bogus 9-1-1 calls. Since PSAPs have no way of determining in advance which calls are real and which are fraudulent, they must answer every call.

A TDoS attack can overload PSAP phone systems to the point where they are incapable of receiving or placing calls. This is a very real threat to PSAP operations. In October 2016, for example, an Arizona teenager was charged with sending thousands of calls to 9-1-1 emergency PSAPs and law enforcement agencies in multiple states using compromised cellphones.[1]

A man-in-the-middle attack is another potential threat for PSAPs, although it is a far lower risk to PSAP operations than DoS and TDoS attacks because most PSAPs use secure Wi-Fi connections within PSAP walls. In a man-in-the-middle attack, attackers use the wireless link between the user device and the cell tower to steal data or monitor conversations.

User and Device Threats

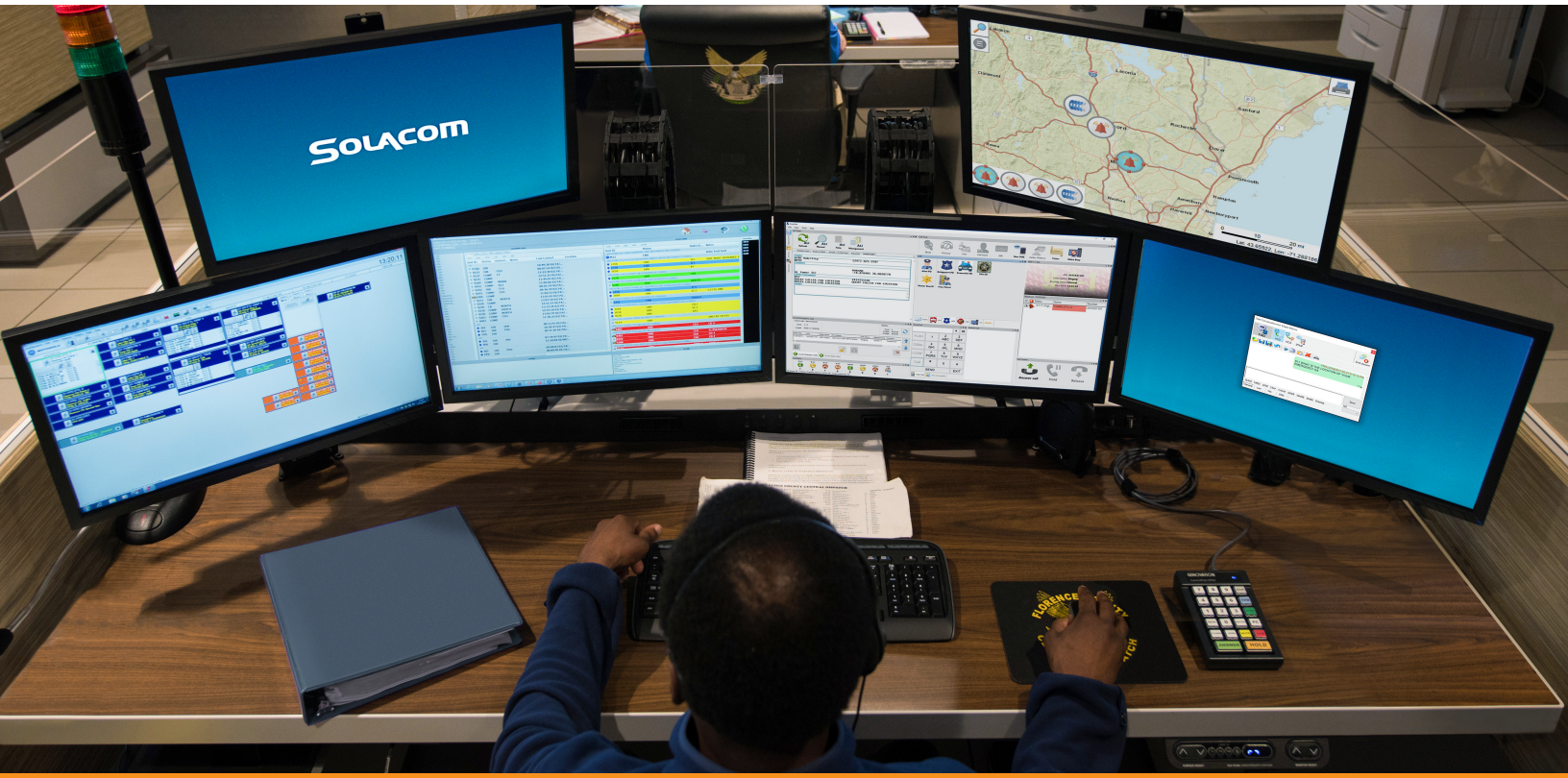
Cyberthreats to users and devices range from continuous pop-ups that slow computer functions and make them difficult to use to data theft and complete loss of control over a computer.

Any computer that is connected to the internet is at direct risk for cyberattacks. This means crucial computer-aided dispatch (CAD) systems are potentially among your most vulnerable. Once hackers gain access to your internet-connected systems, they can potentially access any computer connected to that system. This means call-taker workstations, which typically do not have a direct internet connection, are also at risk.

Hackers are very determined people and they will put in significant effort to gain unauthorized system access. This was proven in August 2017, when Schuyler County in New York experienced a cyberattack where hackers gained access to the communication system for the county through brute force cracking of passwords. The attack temporarily crippled the county's ability to dispatch deputies.[2]

Once hackers gain access to your internet-connected systems, they can potentially access any computer connected to that system. This means call-taker workstations, which typically do not have a direct internet connection, are also at risk.

Ransomware is among the most serious cyberthreats to PSAP users and devices. Ransomware is software that blocks access to computer systems, demanding a ransom be paid to "free" the system. The WannaCry ransomware cyberattack in May 2017 affected more than 200,000 computers running the Microsoft Windows operating system in 150 countries.[3]



Ransomware cyberattacks have also directly targeted PSAPs. In March 2018, Baltimore's 9-1-1 system was held hostage in a ransomware attack that compromised the city's CAD server. The city was forced to shut down its digital dispatch and recording systems for almost 24 hours and revert back to manual dispatching.[4]

Additional threats to users and devices include:

- **Data breaches** that give hackers access to the data on the computer so they can manipulate, corrupt, or steal it.
- **Malware** that is downloaded to the computer for a variety of malicious purposes. Malware can include botnets, viruses, spyware, trojans, and rootkits.
- **Spear-phishing** attacks that use personalized email or social media communications — often by hijacking or mimicking the account of a trusted sender — to persuade people to share confidential information.
- **Spoofing** attacks that enable an unauthorized device to masquerade as an authorized device to access confidential systems and data.
- **Insider threats** from employees or other authorized personnel who steal, corrupt, or destroy data.

Service Threats

Swatting is the main cyberthreat to PSAP services. Swatting is when individuals manipulate IP-based 9-1-1 calls to indicate the call is originating from a location where a very serious criminal act has occurred or is occurring, prompting PSAPs to dispatch a Special Weapons and Tactics (SWAT) team to the call location.

In December 2017, a California man was arrested after he attempted to swat his online video game opponent, but used the wrong address. Instead of his opponent's house, police were sent to an address in a Kansas jurisdiction. When they arrived, a resident at the location tried to understand what happened, but was shot during the confusion.[5]

STEP 2

Evaluate Cybersecurity Requirements

As you evaluate the cybersecurity strategies and solutions needed to mitigate and contain cyberattacks, look at the landscape from two perspectives:

- Network strategies and solutions
- On-premises strategies and solutions

Look at the Network Side

The network side of the cybersecurity equation is managed by your service provider. And it's particularly important as you migrate to ESInets that rely on IP networking technologies to support next-generation core services.

Ask your provider what technologies and processes they have in place to:

- Prevent unauthorized network access
- Determine the origin of cyberattacks, should they occur
- Rapidly escalate response levels to cyberattacks
- Isolate affected component(s) in the network to contain the spread of cyberattacks
- Upgrade or modify network hardware and software to reduce the likelihood of similar attacks in the future

It's also crucial to understand the signs and symptoms of a network-based cyberattack within your operations. Be sure to ask your network service provider what you should look for and who you should contact within their organization if you suspect or detect a cyberattack.

Look at the Premises Side

PSAPs are not typical enterprises. Your call takers and staff rely on your software and systems to respond to matters of life and death around the clock. As a result, the cybersecurity processes and procedures you put in place must be designed to support the unique nature of your operations.

For example, while most enterprises can schedule automated software updates and patches for workstations and systems, PSAPs must adopt a far more controlled approach. The consequences could be disastrous if a call taker's workstation automatically reboots to apply a software update during a 9-1-1 call, or a dispatch request is lost because a patch is being applied to CAD software.

PSAPs also need a more rigorous approach than standard enterprises for dealing with failed software updates and patches. While it's inconvenient for any employee to be without a workstation for an extended period of time, the downtime is far more detrimental in a PSAP where public safety is at stake.

Along with requirements for software updates and patches, it's also important to consider cybersecurity requirements in the context of how the workstation or computer is used. For example:

- Workstations and servers that are directly connected to the internet are at the highest risk for cyberattacks, so they will likely require more frequent security updates than computers that are not directly connected to the external network.
- Open ports on servers are a point of vulnerability, so it's very important that servers are hardened to ensure that only the appropriate server ports are left open.
- USB ports on computers are another point of vulnerability, so it may make sense to prevent connection of portable storage devices.

While the majority of PSAPs already have an off-site backup location as part of their business continuity plan, it's important to ensure the backup site uses different servers and workstations than those at the primary site. When primary and secondary sites contain identical equipment, there is greater likelihood that both sites will be affected by a cyberattack.

In addition, the processes and procedures required to quickly and securely shift operations to the backup site then back to the primary site once conditions allow it are often different in the case of a cyberattack than in the case of other unplanned events, such as severe weather. As a result, business continuity plans should include contingencies for incident response plans, restoration of critical systems, and return to standard operations that are specific to cybersecurity attacks.

Other must-haves for on-premises cybersecurity include:

- Computer and internet usage policies
- Training in safe cybersecurity practices for all staff
- Authentication mechanisms for system and network access
- Data encryption
- Regular audits of cybersecurity measures and processes
- Audit logs

Consult Available Resources

NENA is an important source of information to learn more about cybersecurity requirements in PSAPs and best practices for business continuity. Among other items, the NENA Interconnection and Security Committee oversees the technical integration and operational impacts of existing and new security technologies on an overall system.

In addition, documents such as the NENA Communications Center/PSAP Disaster and Contingency Plan Model Recommunication provide guidance and recommendations for disaster and contingency plans for:

- IT security
- Telephone services
- Public safety radio networks
- CAD systems

The document also includes checklists for DoS attacks against PSAPs and for return to normal operations.

STEP 3

Engage With NG9-1-1 Cybersecurity Experts

With the expertise and cost required to develop, implement, and maintain a comprehensive cybersecurity strategy, it often makes sense for PSAPs to partner with NG9-1-1 cybersecurity experts. Few PSAPs have the specialized cybersecurity knowledge and experience necessary in-house.

For many PSAPs, a managed services offering from an NG9-1-1 system vendor is the best approach to cybersecurity. NG9-1-1 experts bring PSAPs far more relevant knowledge and understanding of PSAP and public safety considerations, approaches, and technologies than a general-knowledge cybersecurity partner can. With an industry partner, key cybersecurity capabilities are built into systems and services for NG9-1-1 emergency call handling and management.

Solacom Is Ready to Help

Solacom understands the cybersecurity threats PSAPs face, as well as the technologies and solutions required to mitigate and contain cyberattacks.

Our Guardian Managed Services ensure the Solacom Guardian 9-1-1 solution is always operating at peak performance. Active remote monitoring services ensure all alerts are investigated by certified Solacom technicians who are trained to monitor the health of the emergency call management solution, analyze performance, and interpret alarms.

A managed services offering from an NG9-1-1 system vendor is the best approach to cybersecurity. NG9-1-1 experts bring PSAPs far more relevant knowledge and understanding of PSAP and public safety considerations, approaches, and technologies than a general-knowledge cybersecurity partner can.

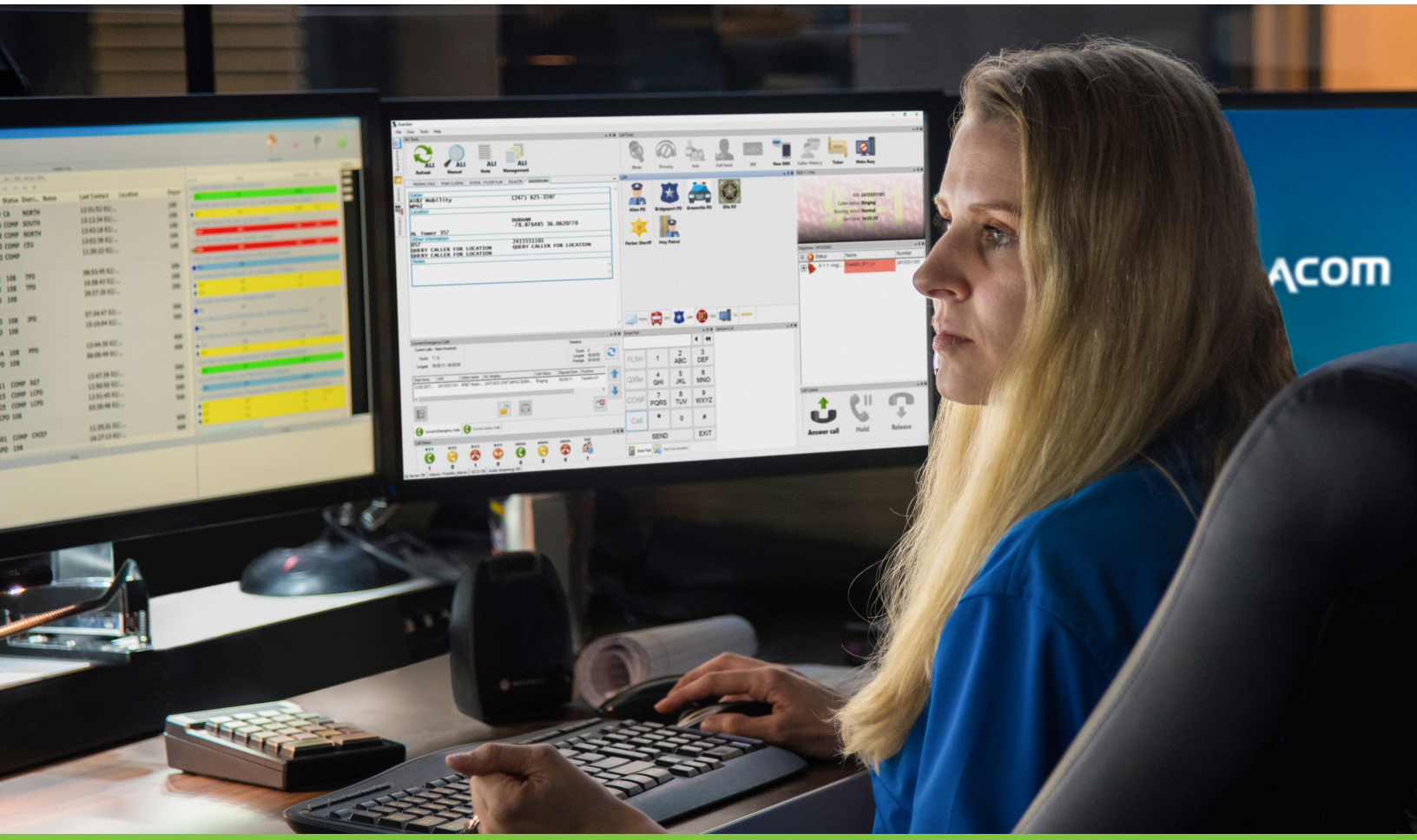
In addition, we maintain all factory-installed protection systems remotely and ensure the latest updates are tested and verified before they are installed. This includes:

- Real-time anti-virus and anti-malware detection and removal engines
- Phishing protection
- Spam guard
- System performance optimizer
- File encryption
- Multiple scan levels
- Two-way firewall
- Identity theft protection
- USB immunizer, which immunizes flash drives from virus infections when connected to a computer

Our disaster recovery services provide additional peace of mind by making full copies, or snapshots, of system data and configuration details to protect the emergency call management infrastructure, should unexpected events occur.

Solacom also provides equipment such as firewalls and session border controllers (SBCs) that help protect PSAP systems from cyberattacks. And we have developed proven processes and rules for server hardening and workstation lockdown to restrict the actions that can be taken on these devices and help protect systems within the PSAP premises.

As we evolve our offerings, we will continue to enhance our capabilities with additional cybersecurity monitoring and management services to help PSAPs mitigate the risks associated with cyberattacks.



Additional Information

Click here for more information about the advanced NG9-1-1 system monitoring and management services provided with Solacom Guardian Managed Services.

Contact Us

Solacom 9-1-1 call handling and management solutions are built on more than 30 years of research and innovation in the application of advanced hardware and software technologies for public safety. Today, Solacom Guardian 9-1-1 solutions support thousands of agencies affecting millions of lives annually — from dense urban environments to statewide deployments.

Contact us today to discover how our Guardian solutions can help your PSAP streamline 9-1-1 call handling and management processes and enable more efficient collection of critical information in emergency situations.

Visit our website: www.solacom.com

References

[1] http://nymag.com/selectall/2017/03/how-a-viral-tweet-overwhelmed-the-nations-911-call-centers.html
[2] https://www.fortr3ss.com/2017/09/27/hacking-of-upstate-police-prove-the-need-for-stronger-cyber-security/
[3] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[4] http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-hack-folo-20180328-story.html
[5] https://www.cnn.com/2017/12/30/us/kansas-police-shooting-swatting/index.html

SOLACOM