adNET
Technology Management

A GUIDE TO SAFE IT PRACTICES FOR FIRE DEPARTMENTS AND DISTRICTS:

EIGHT TECHNOLOGICAL PITFALLS THAT CAN DAMAGE YOUR FIRE DEPARTMENT OR DISTRICT—AND HOW TO AVOID THEM

Modern fire departments and fire services rely on computer technology more than ever. Whether it's facilitating communication through reliable VoIP services, recording call data, interacting with emergency vehicles and teams in the field via GPS, or staying apprised of the relevant ongoings in the local area, the need for smooth operations is huge.

Unfortunately, many cybercriminals know that fire departments and districts safeguard a host of valuable protected information and will prey on vulnerable fire departments with phishing scams, ransomware, and a range of other cyberattacks. Consequently, maintaining a robust IT infrastructure that strategizes based on the unique needs of a fire department is essential.

Our specialized guide can help your department or district develop and implement a more secure IT strategy by pinpointing eight of the most common technology pitfalls for fire departments and providing suggestions for how to avoid them.

1. YOU DON'T HAVE A CYBERSECURITY PLAN

While cybersecurity remains an issue for businesses across all industries, the fire safety sector is perhaps at even greater risk than most. Fire rescue teams collect and store thousands of files of medical data, and

WE DON'T JUST MODERNIZE YOUR IT INFRASTRUCTURE WITH UP-TO-DATE SYSTEMS AND PROTECT YOU FROM SECURITY THREATS AND PRODUCTIVITY HICCUPS— WE HELP YOU PLAN FOR THE FUTURE.

Call us at (877) 264-2968 or email us at info@adnet.us.

For more information, visit our website at **www.adnet.us**.

departments have to take careful steps to ensure that this information remains protected, not only for the safety of private citizens but also to stay compliant with HIPAA regulations.

Cyberattackers understand the value of medical records and the lengths organizations must go to in order to protect them, which has led fire departments to become a primary target for hackers. Without a cybersecurity plan, opportunistic cybercriminals will use hacking scams to infect systems with ransomware, which can prevent access to key files until a ransom is paid. Meanwhile, phishing scams can access the fire department's financial accounts while additionally slowing the performance of computers with other viruses.

Hackers are bound to attack fire departments whose protected health information is vulnerable, which can have detrimental monetary and legal consequences for your department.

2. YOUR CURRENT IT STAFF HAS SLOW RESPONSE TIMES

Most businesses live by the mantra that time is money. For fire departments, though, time is far more important than money. It could mean the difference between being able to save lives or not. As such, poor response times from your IT team can severely compromise your ability to provide the level of service that emergency situations require.

1 | SUGGESTIONS:

For the safety of your organization and the citizens in your local area, it's crucial that your department or district implement a cybersecurity plan that is well-equipped to protect against cyberattacks that commonly impact organizations in the fire fighting industry.

Your IT plan should include a strategy for how to detect vulnerabilities in your systems and practices and address them to protect against potential threats. In order for your department to meet HIPAA and other security regulations, your cybersecurity plan needs to extend beyond simply installing antivirus or anti-malware software. A Managed IT Service Provider (MSP) who specializes in cybersecurity for fire departments and districts, such as adNET Technology Management, can help your department develop an IT plan and implement cybersecurity policies that are strategized according to the unique needs of your department.

Beyond emergency instances, even the day-to-day processes of your fire department are heavily reliant on the speed of your IT responses. Whether it's due to inadequate systems, unreliable connections, poor notification facilities, or insufficient staff input, those delays can spell disaster. Too few IT specialists or IT providers who are difficult to get ahold of simply cannot provide the adequate IT solutions a fire department needs.

3. YOUR DEPARTMENT HAS NOT UPGRADED TO THE LATEST TECHNOLOGIES

Technology has become pivotal in the operations of most fire departments and related industries. It's not unlikely that your fire service uses tech devices and software in virtually every aspect of business. However, technology evolves at a rapid rate, and persisting with older systems and software can cause serious damage. Aside from time delays, outdated systems can lead to compatibility issues when trying to implement new applications or programs. Likewise, failing to update your IT infrastructure can leave the department open to the newest forms of ransomware.

Keeping your technology updated is crucial not only to operations at the fire station but also to firefighters on duty. Regular equipment such as firefighting drones, modern radio communication, fire pumps,

2 | SUGGESTIONS:

Immediate attention to your department's IT issues should be a top priority for your IT provider. Your department should never have to sacrifice quick emergency response times because your IT provider's response times are too slow. Our teams at adNET specialize in fire department security and understand that emergency IT solutions are a necessity in this industry. We guarantee quick services when you're in need to ensure your IT aids instead of hinders crucial operations.

Our experts are also dedicated to identifying and treating underlying issues before they cause downtime or delays, which prevents many IT disasters from occurring and ensures your tech is ready when you need it most. Just like you, we're used to putting out fires, but we'd rather prevent IT fires than put them out. That's why we take precautions to ensure your systems are protected before major issues can occur.

and personal protective equipment often interact with technology at the fire station or in the emergency vehicle. In-helmet thermal imaging displays and personal location equipment are also very common items that can transform the performance of your service and the safety of the firefighting experts. Without an updated IT infrastructure, your department's operations both at the station and in the field can be jeopardized.

4. YOUR DEPARTMENT'S IT IS NOT HIPAA COMPLIANT

As previously mentioned, fire departments are required to adhere to the same HIPAA rules and regulations as hospitals and other healthcare facilities. HIPAA regulations outline cybersecurity measures that must be taken in order to avoid data breaches of PHI, or protected health information. Not following these regulations could land your department in legal and financial trouble.

Thus, since fire departments are responsible for the protection of confidential personal data including social security numbers and patient medical histories, maintaining HIPAA compliant IT infrastructures is absolutely critical. Otherwise, your department may face financial fines of up to $1.5m while also experiencing a host of other logistical damages and loss of trust.

3 | SUGGESTIONS:

In addition to analyzing the condition of your current infrastructure and its ability to evolve with advancing technology, you should invest in software specialized for fire departments, such as RescueNET, FireHouse Manager, and FIREHOUSE Software. These softwares do everything from preventing you from leaving patient care reports uncompleted, to tracking PPE and inspections, to planning field operations.

Though upgrading to new software can be a complex process, using an outsourced, fire department–focused MSP ensures these softwares are installed, updated, and monitored frequently and that your department operations aren't delayed during the rollout of a software upgrade.

4 | SUGGESTIONS:

Use an IT provider that boasts vast knowledge of HIPAA requirements to ensure your department remains compliant at all times. Because these regulations are often updated, using IT personnel who don’t specialize in cybersecurity legal requirements will likely lead to your IT practices falling out of compliance.

With an MSP like adNET, you’re guaranteed a team of IT experts whose job is to remain educated on HIPAA compliance and other security regulations. Our teams can strategize your IT practices according to these rules to ensure your data remains protected and your department avoids legal and financial consequences.

5. YOUR PROVIDER FAILS A COST-BENEFIT ANALYSIS

Many fire departments contract IT specialists as needed or rely on one IT specialist to handle every IT need, from servers, to network connection, to data warehouses. While these are not only far too many tasks for one IT specialist to handle effectively, it will likely be very costly and inefficient to hire different specialists to complete each task as it arises.

By waiting for problems to arise before you hire a specialist, you spend more out of pocket and must wait for contractors to respond to your service request. While having an IT specialist on-hand at all times is preferrable, it will still be overwhelming for a single IT manager to handle all the tasks necessary for your departments IT to function smoothly and avoid downtime.

Fire tech and equipment is expensive and complex. So if your provider isn’t maintaining a high standard for IT functionality and efficiency, they aren’t worth the time and money.

6. YOUR IT SPECIALISTS AND OTHER VENDORS AREN’T COLLABORATING

As you know from your in-house endeavors, smooth communication across various departments is vital. Your fire department often needs to meet obligations that cross over to other departments, services, and vendors, so similarly, your IT specialists need to be invested in collaborating with your partner entities.

Failure by your IT personnel to communicate with any necessary organizations—whether directly connected to your department or not—can seriously hinder the speed of the operation while also leaving boxes unchecked and affected parties unnotified. This lack of transparency and collaboration simply cannot be afforded by fire departments who need to be ready to respond to emergencies at a moment's notice.

7. YOUR DEPARTMENT IS SPENDING TOO MUCH TIME RESOLVING IT PROBLEMS

For departments whose IT team is small or lacking resources, when IT issues arise, your department is likely spending more staff time than necessary to resolve them. Spending excess amounts of time fixing IT issues usually results in longer periods of downtime, which can have serious impacts on your department's functionality.

Because smaller IT teams tend not to have the time or resources necessary to implement preventative measures for potential IT issues, problems are more likely to occur and your overall productivity rates to decrease. Even more disconcerting is that greater levels of downtime

5 | SUGGESTIONS

Outsourcing your IT management to a fire department–focused MSP helps you meet both your budgetary needs as well as your IT requirements. At adNET, total managed services cost as little as one salaried employee, meaning you get the resources and expertise of a whole team of fully equipped IT professionals for the cost of just one IT specialist.

Outsourcing to adNET will also allow you to leverage success from our experts' knowledge of the industry while also ensuring that every decision pertaining to your IT infrastructure is scrutinized. We guarantee services such as fire department software implementation, system reconfiguration when necessary, and IT responses in faster times and at a better price.

6 | SUGGESTIONS

When seeking an IT specialist for your fire department or fire district, be sure to choose a service provider who is dedicated to working alongside the various vendors and partners across the district. As MSPs offer collaboration with your partners as an integrated service, your department can rest assured that the correct parties are being informed of real-time issues involving your IT.

and time spent fixing issues can prevent important messages from being relayed between firefighters and other personnel and could even result in catastrophic loss of lives in emergency situations.

8. YOU DON'T HAVE AN IT STRATEGY OPTIMIZED FOR FIRE DEPARTMENTS AND DISTRICTS

Finally, a lot of departments working in the fire rescue industry will assume that non-specialized IT providers will adequately serve their IT needs. However, while the principal services of IT remain the same across all industries, the mechanisms, methods, and protocols implemented for each industry's unique IT strategy vary significantly.

Opting for a non-specialized IT provider means you'll be offered generic solutions that might not be the most beneficial for your unique organization. Specialized MSPs provide services that ensure all legal, financial, and functional obligations are met and that align with your organization's goals and strategies.

7 | SUGGESTIONS

Hiring an MSP that specializes in working with fire departments and treating the underlying issues in a proactive manner puts the whole network on smoother ground, causing fewer issues to occur. Rather than using full-time staff's valuable time to resolve IT problems, you can rely on a well-trained team of experts to use their own time and resources to address and prevent issues for you. That way, your team can stay focused on their important job duties and tasks.

8 | WHAT YOU CAN DO NOW:

Using adNET as your IT partner is the perfect solution. Aside from being focused on the specific challenges faced by the fire service, we offer a full audit and consultation service to discuss the obstacles and objectives of your specific department or district. We don't just modernize your IT infrastructure with up-to-date systems and protect you from security threats and productivity hiccups—we help you plan for the future.

Contact adNET Technology Management today to speak with one of our IT service experts.

Call us at (877) 264-2968 or email us at info@adnet.us.

For more information, visit our website at **www.adnet.us**.