ASK Technologies, Inc.

WINTER 2017

Volume 17 Issue 1

ASK NEWS

In this edition of ***ASK News***, it is all about mitigating risk and increasing security. We explore the most up to date information on Ransomware, software licensing compliancy, and discuss our latest product and services offering, Video surveillance and security products in the workplace. Enjoy the read.

Stephen Pirolli, ASK Technologies, Inc.

Inside this issue:

WELCOME NEW CLIENTS

Microsoft Innovation Center

KEYSTONE

CompuData

Ransomware Today

From our Sales Team

More and more, ransomware has emerged as a major threat to individuals and businesses alike. Ransomware, a type of malware that encrypts data on infected systems, has become a lucrative option for cyber extortionists. When the malware is run, it locks victim's files and allows criminals to demand payment to release them. Organizations of all types and sizes have been impacted, but small businesses can be particularly vulnerable to attacks.

Ransomware is distributed in a variety of ways and is difficult to protect against because, just like the flu virus, it is constantly evolving.

How Ransomware Is Spread

Spam is the most common method for distributing ransomware. It is generally spread using some form of social engineering; victims are tricked into downloading an e-mail attachment or clicking a link. Fake email messages might appear to be a note from a friend or colleague asking a user to check out an attached file, for example. Or, email might come from a trusted institution (such as a bank) asking you to perform a routine task. Sometimes, ransomware uses scare tactics such as claiming that the computer has been used for illegal activities to coerce victims. Once the user takes action, the

continued on pg. 2

Protect Your Premises: Surveillance & Security

From our Sales Team

Security and surveillance is a priority for every business, but finding the right solution can be confusing. You don't want something that's too big and complex to manage. However, you still need a solution that's smart enough to do the job.

Everything you need from one supplier

Our solutions are designed for businesses just like yours. So, you can solve problems such as protecting staff, premises and assets, while still focusing on your core business. They're easy to install, use and maintain. And as your needs grow, you can grow your ***ASK***/Axis system too. It's a safe investment that provides everything you need to support your operations – all from one supplier.

A complete system, for total control

If you're looking for a complete solution that can cover all your surveillance

continued on pg. 4

Software Audits: 7 Hidden Compliancy Risks

as featured on CIO.com

Software companies turning up the heat on licensing audit activity, especially on enterprise customers. A survey from 1E reveals that the average number of software vendor audits is now four per year. For 10 percent of U.S. companies surveyed, the number jumps to between 11 and 15 per annum.

It's not just the volume that's on the rise; it's also the intensity. For many vendors, the "tone" of auditing activities has shifted from let's-make-this-right to downright aggressive. Take recent changes to IBM's audit clause. As noted by Gartner, the vendor has removed language saying audits will be conducted in a way that minimizes disruption to the customer's business activities.

The change in attitude stems in part from the growing pains happening as traditional on-premise software vendors find their footing (and adjust to different revenue patterns) in the cloud. For some, it's a matter of expediting adoption of new cloud services. Penalties for a non-compliant customer may be waived if the client upgrades to cloud services.

continued on pg. 4

Ransomware Today

continued from pg. 2

malware installs itself on the system and begins encrypting files. It can happen in the blink of an eye with a single click.

Another common method for spreading ransomware is a software package known as an exploit kit. These packages are designed to identify vulnerabilities and exploit them to install ransomware. In this type of attack, hackers install code on a legitimate website that redirects computer users to a malicious site. Unlike the spam method, sometimes this approach requires no additional actions from the victim.

Protect Against Ransomware

Cyber criminals armed with ransomware are a formidable adversary. While small-to-mid-sized businesses aren't specifically targeted in ransomware campaigns, they may be more likely to suffer an attack. Frequently, small business IT teams are stretched thin and, in some cases, rely on outdated technology due to budgetary constraints. This is the perfect storm for ransomware vulnerability. Thankfully, there are tried and true ways to protect your business against ransomware attacks. Security software is essential, however, you can't rely on it alone. A proper ransomware protection strategy requires a three-pronged approach, comprising of education, security and backup.

Education: First and foremost, education is essential to protect your business against ransomware. It is critical that your staff understands what ransomware is and the threats that it poses. Provide your team with specific examples of suspicious emails with clear instructions on what to do if they encounter a potential ransomware lure (i.e. don't open attachments, if you see something, say something, etc.).

Conduct bi-annual formal training to inform staff about the risk of ransomware and other cyber threats. When new employees join the team, make sure you send them

continued on pg. 3

These ransomware spam campaigns are operating on a massive scale.

The malware is spread using spam, typically in the form of an email message disguised as an invoice.

When opened, the invoice is scrambled and the victim is instructed to enable macros to read the document.

Ransomware Today

continued from pg. 2

an email to bring them up to date about cyber best practices. It is important to ensure that the message is communicated clearly to everyone in the organization, not passed around on a word of mouth basis. Lastly, keep staff updated as new ransomware enters the market or changes over time.

Security: Antivirus software should be considered essential for any business to protect against ransomware and other risks. Ensure your security software is up to date, as well, in order to protect against newly identified threats. Keep all business applications patched and updated in order to minimize vulnerabilities.

Some antivirus software products offer ransomware-specific functionality. Sophos, for example, offers technology that monitors systems to detect malicious activities such as file extension or registry changes. If ransomware is detected, the software has the ability to block it and alert users.

However, because ransomware is constantly evolving, even the best security software can be breached. This is why a secondary layer of defense is critical for businesses to ensure recovery in case malware strikes: backup.

Backup: Modern total data protection solutions, like Datto, take snapshot-based, incremental backups as frequently as every five minutes to create a series of recovery points. If your business suffers a ransomware attack, this technology allows you to roll-back your data to a point-in-time before the corruption occurred. When it comes to ransomware, the benefit of this is two-fold. First, you don't need to pay the ransom to get your data back. Second, since you are restoring to a point-in-time before the ransomware infected your systems, you can be certain everything is clean and the malware can not be triggered again.

Additionally, some data protection products today allow users to run applications from image-based backups of virtual machines. This capability is commonly referred to as "recovery-in-place" or "instant recovery." This technology can be useful for recovering from a ransomware attack as well, because it allows you to continue operations while your primary systems are being restored and with little to no downtime. Datto's version of this business-saving technology is called Instant Virtualization, which virtualizes systems either locally or remotely in a secure cloud within seconds. This solution ensures businesses stay up-and-running when disaster strikes.

Conclusion

Cyber extortionists using ransomware are a definite threat to today's businesses from the local pizza shop to the Fortune 500. However, a little bit of education and the right solutions go a long way. Make sure your employees understand what to watch out for and you can avoid a lot of headaches. Never underestimate the dedication or expertise of today's hackers. They are constantly adapting and improving their weapon of choice. That's why you need top-notch security software and backup. Keep your business safe and give your nerves a break.

To sum it all up, Knowledge spreading and security software can help you avoid cyberattacks. Patch management is essential. Be certain that your software is up-to-date and secure. And in the end, it is backup that will help you pick up the pieces when all else fails.

Consider using a modern backup product, such as one offered by Datto, with features that can permanently eliminate downtime. Contact your local ***ASK Sales Rep*** for more information, by calling (610) 617-0300.

Downtime from ransomware costs small businesses $75B EACH YEAR, or roughly 300,000 roundtrips to outer space aboard the Virgin Galactic SpaceShipTwo.

With a Datto backup and recovery solution, 97% of small businesses infected fully recovery with minimal downtime.

datto
PARTNER PLUS

Premier
PARTNER

Protect Your Premises: Surveillance & Security

continued from pg. 1

needs, look no further than an ***ASK***/AXIS Camera Station video management software. It helps you handle incidents effectively and export high-definition evidence, quickly.

You can also add extra features, so you can communicate with visitors, secure entrances and exits, handle goods deliveries and use audio for deterrence. You can even use analytics on your camera to further enhance system performance.

It's the perfect match for Axis' wide range of products. A range that includes 4K Ultra HD cameras, thermal cameras and products for harsh and hazardous environments – and much more.

Stay safe and secure

With ***ASK***/Axis, you won't just get the right system to suit all your needs; you'll also get value for money and first-class support. We offer intelligent security solutions that enable a smarter, safer world. And as the market leader in network video, Axis is driving the industry by continually launching innovative network products based on an open platform - delivering high value to customers through a global partner network.

Whatever ***ASK***/Axis system you choose, you can rely on the best performance, all day, every day. And, as the needs of your premises grow or change, you can extend it quickly and easily. So, you can rest assured your business will be well protected.

Contact your local ***ASK Sales Rep*** for more information, by calling (610) 617-0300.

Everything You Need

- ***Video – for clear images***
- ***Access control – for secure premises***
- ***Audio – for communication***
- ***Visitor management – for extra security***
- ***Control - for integration with other devices***

Software Audits: 7 Hidden Compliancy Risks

continued from pg. 2

Penalties for a non-compliant customer may be waived if the client upgrades to cloud services. For others, it's an effort to supplement declining on-premise license and maintenance revenues.

The problem with non-compliance is that it's typically obscured. Few enterprises knowingly engage in improper license use – but most would be found out of compliance if they underwent a major IT vendor audit. The most common reasons are:

1. *You bought software for one reason, now you use it for another.* Certain license types, such as limited use licenses, can only be used in non-production environments like development, testing or failover. Companies often purchase these licenses rather than full use licenses to obtain a pricing discount. Then, months or years later they discover their limited use licenses are being used for production use purposes like internal data processing operations.

2. *No one told you the product use rights changed.* Product use rights can change at any time, and the rate of change is growing among larger IT vendors. For example, during recent contract negotiations and audits, SAP and Oracle have begun to ask clients to purchase additional licenses for third-party application access. A business with 100 Salesforce.com licenses that need to access information from SAP may now be required to buy 100 additional licenses. It's only been in the last few years that vendors have begun to interpret "indirect access" this way and attempted to enforce it with clients.

continued on pg. 5

"Few enterprises knowingly engage in improper license use – but most would be found out of compliance if they underwent a major IT vendor audit."

Software Audits: 7 Hidden Compliancy Risks

Continued from Page 2

3. *Your definition is different from the vendor's.* Licensing programs and definitions have changed dramatically. What constitutes a qualified user or device (Microsoft)? What about a concurrent user or a floating user (IBM)? What's the difference between an application-specific full-use license or an embedded software license (Oracle)? Any misinterpretation can unwittingly throw a customer out of compliance.

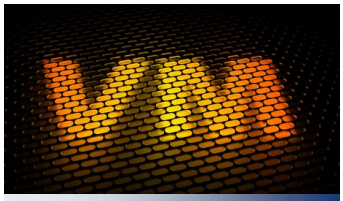
4. *You upgraded your software/hardware.* Or maybe you downgraded. If you upgrade or downgrade your software, which product use rights apply – the rights that came with your original purchase, or the rights that came with your up/downgrade? How will your support and maintenance agreement be impacted? Well, it varies and it can be confusing, depending on your vendor. Did you recently upgrade mainframe or server hardware? Often, that means additional MIPs or cores that will also be require to buy software licenses for whether you use them or not.

5. *Virtualization.* Virtualized environments are hotbeds for unintentional non-compliance as each vendor has very specific rules around how hosts and software are coupled and managed. For example, let's say you have two physical Microsoft Windows Servers (2012), with two virtual sessions running on each. Using VMware's tools, you move one virtual session from one server to the other. Soon thereafter, you want to move it back again. Unfortunately, Microsoft doesn't allow "server mobility" beyond the first move. The virtual session can move one time (in this case from the first server to the second), but is then stuck on the second server for 90 days. In this instance, this is ground for non-compliance as Microsoft requires a new license to run three (rather than two) virtual sessions on one machine.

6. *You unknowingly purchased software licenses from an ISV.* More companies are turning to independent software and technology vendors for complex, industry-specific IT solutions (e.g., diagnostic equipment in healthcare, production floor technologies in manufacturing). In some cases, these solutions contain third party software that isn't disclosed to the buyer and, therefore, isn't on your asset management radar screen.

7. *You don't have a formal process and tools for distributing, licensing and*

continued on pg. 6



"Virtualized environments are hotbeds for unintentional non-compliance as each vendor has very specific rules around how hosts and software are coupled and managed."

CLIENT QUOTE

"Hi Steve,

…You, Steve Callahan, Geoff Smith, Dave Livingston, and others on the team, did an excellent job for us [replacing our servers and converting our applications]. I really appreciate all of your hard work. Everything is going really well up here. The next time you come up, Jim and I will give you some snacks (Pirate Booty) or whatever you want… Thanks again!"

Dianne Brodt, Assistant Manager
Keystone Food Products, Inc., Easton, PA

ASK Technologies, Inc.

7 Bala Avenue
Suite 201

Bala Cynwyd, PA 19004

610-617-0300 Office
610-617-0307 Fax
info@asktech.com

*For operational excellence at predictable costs, turn to **ASK**.*

SHORT CUTS
New for Windows 10

Windows + M
Minimize all windows

Windows + S
Open search

Windows + I
Open settings

Windows + ,
Temporarily peek at the desktop.

Ctrl + F4
Close the active window

Ctrl + Esc
Open the start menu

ASK TECHNOLOGIES, INC.

Creating new standards in multi-service network integration.

Why Should I Upgrade to Windows 10?

as featured on theguardian.com

Embraced warmly after Vista, Win7 has remained a popular favorite as Windows 8 and 8.1 came and went. Windows 10 is a worthy successor, yet many users cling to Windows 7.

Depending on your hardware, a straight upgrade from Windows 7 to 10 may offer some benefits. These start with smoother and sometimes faster operations, more economical use of memory and disk space, increased security, and the integration of OneDrive cloud storage.

File Explorer is a better file manager, and DirectX 12 promises better gaming. Task View makes it easier to access running programs. Virtual desktops, which were easily added, are now built in. The system refresh and reset options make it simpler to maintain your PC.

Windows 10 also includes the new Edge browser, though IE11 is still there, hidden away. You can also search the internet from your desktop.

Further, Windows 10 provides better built-in support for newer types of hardware including secure boot capabilities with UEFI, USB 3.0, Bluetooth adapters, high-definition screens, and solid state drives.

If you are still reluctant to migrate your business workstations and notebooks to Window 10, there is good news. Microsoft doesn't plan to stop fixing security problems in Win7 until the extended support ends. That doesn't happen until January 14, 2020--five years and a day from the end of mainstream support. So you still have some time.

Contact your local ***ASK*** Sales Rep for help migrating to Windows 10 by calling (610) 617-0300.

Software Audits: 7 Hidden Compliancy Risks

Continued from Page 5

managing licenses. Large enterprises often engage in checkbox license management. They invest in software asset (or license) management tools that provide limited auditing capabilities and limited visibility into license usage, and call it a day. Unfortunately, effective management of software licenses requires dedicated people and processes that ensure a 360-degree view and control over how licenses are purchased, distributed, harvested, archived and retired. As the complexity of IT and IT contracting increases, the need for formal asset and license management programs within the enterprise will become even more imperative.

There is no reason to believe that IT vendor audit activity will lessen any time soon. The pressure for old guard vendors to quickly evolve their business to align with a cloud-first landscape is at an all-time high. License audits will continue to play a critical role in revenue generation during that evolution. Enterprises need to understand where their compliance risks are – from the obvious to the hidden.

Conducting self-audits is one great way to find and fix problems before vendors even knock on the door. Mitigation can range from purchasing additional licenses (in a planned, budgeted way), making technology changes to eliminate licensing gotchas, making usage changes to eliminate non-compliance, and considering replacement technologies for elements of the estate.