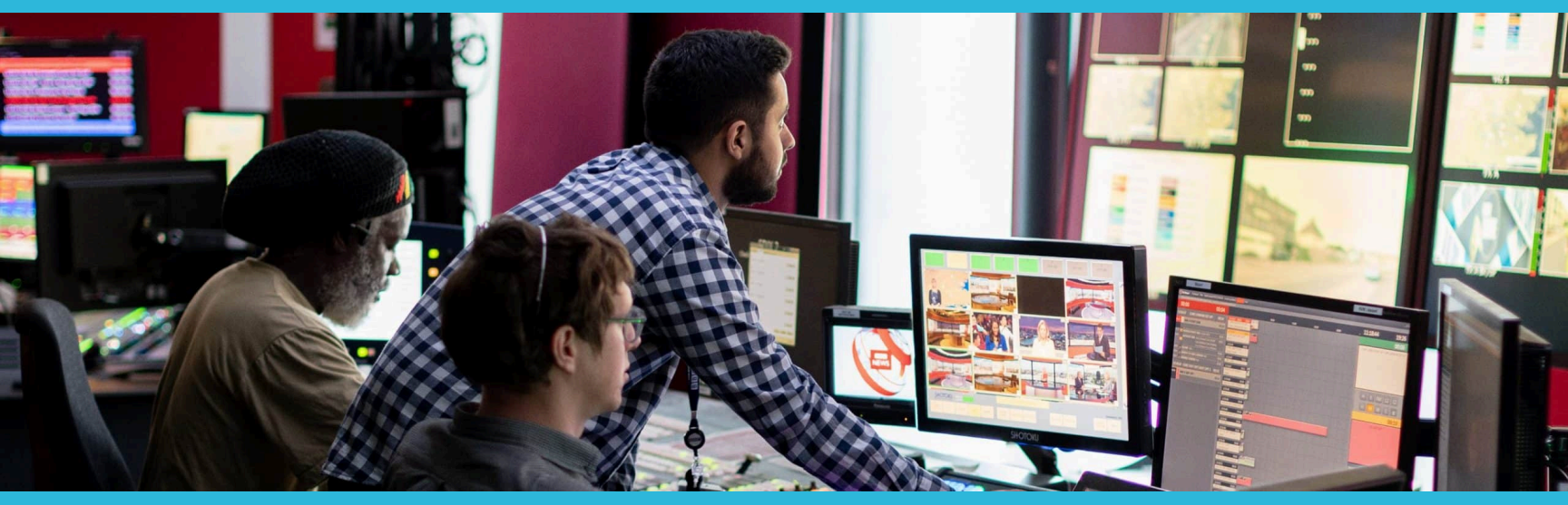
VOLUME 22
NOVEMBER, 2022
CHESHIRE, CT 06410

BlueCastle IT SOLUTIONS



TECH TALK

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

Simple Guide for Better Endpoint Protection	Page 1	Security Tips for Online Holiday Shopping	Page 2
Gadget of The Month	Page 1	Tech Tip of The Month	Page 2
How to Stop Insider Threats	Page 2	VoIP Features for Small Businesses	Page 2
Meet Microsoft Viva Sales	Page 2	Technology Trivia	Page 2

We love technology and we love helping people. Give me a call today for a quick chat to find out how my team and I can help you secure your data better!

– Diana Scott

Owner – BlueCastle IT Solutions LLC

GUIDE FOR BETTER ENDPOINT PROTECTION

Endpoints are the collection of computers, mobile devices, servers, and smart gadgets that make up your company's network and IT infrastructure.

Each of those devices is a chance for a hacker to penetrate a company's defenses.

64% of organizations have experienced one or more compromising endpoint attacks.

The following solutions are focused on the protection of endpoint devices.

Address Password Vulnerabilities

Passwords are one of the biggest vulnerabilities when it comes to endpoints.

Poor password security and breaches make credential theft one of the biggest dangers to cybersecurity.

Address password vulnerabilities in your endpoints by:

- Training employees on proper password creation and handling
- Look for passwordless solutions, like biometrics
- Install multi-factor authentication (MFA) on all accounts

Stop Malware Infection Before OS Boot

USB drives (also known as flash drives) are a popular giveaway item at trade shows.

But an innocent-looking USB can actually cause a breach.

Hackers can use them to gain access to a computer is to boot it from a USB device containing malicious code.

There are certain precautions you can take to prevent this from happening.

One of these is ensuring you're using firmware protection that covers two areas: **Trusted Platform Module (TPM)** and **Unified Extensible Firmware Interface (UEFI)** Security.

TPM is resistant to physical tampering and tampering via malware.

It looks at whether the boot process is occurring properly and also monitors for the presence of anomalous behavior.

Additionally, seek devices and security solutions that allow you to disable USB boots.

Update All Endpoint Security Solutions

You should regularly update your endpoint security solutions. It's best to automate software updates if possible so they aren't left to chance.

Firmware updates are often forgotten about.

But they are just as important for ensuring your devices remain secure and protected.

Use Modern Device & User Authentication

How are you authenticating users to access your network, business apps, and data?

If you are using only a username and password, then your company is at high risk of a breach.

Use two modern methods for authentication:

- Contextual authentication
- Zero Trust approach (Trust but Verify)

Apply Security Policies Throughout the Device Lifecycle

From the time a device is first purchased to the time retires, you need to have security protocols in place.

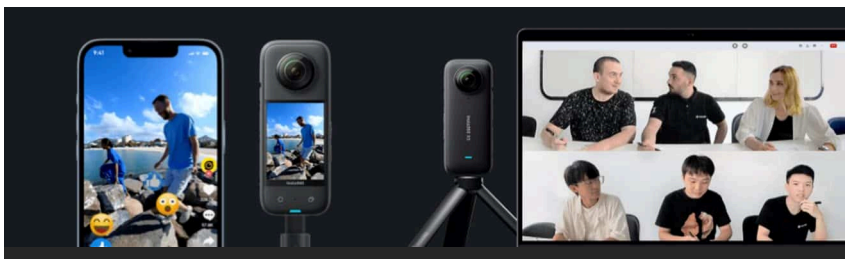
Examples of device lifecycle security include when a device is first issued to a user. This is when you should remove unnecessary privileges.

When a device moves from one user to another, it needs to be properly cleaned of old data and reconfigured for the new user.

When you retire a device, it should be properly scrubbed.

Prepare for Device Loss or Theft

Unfortunately, mobile devices and laptops get lost or stolen. When that happens, you should have a sequence of events that can take place immediately. This prevents company risk of data and exposed business accounts.



INSTA 360 X3 ACTION CAM

Share live moments with 360 Live Streaming

Give your audience the freedom of choice! Just set X3 down and start streaming in 360. Live stream everything around you and let your audience take it all in.

Conference ready with Webcam Mode

Who says you have to sit next to each other during an online meeting? Webcam mode captures everyone in 360. No more huddling in front of a tiny webcam to fit in!

VOLUME 22
NOVEMBER, 2022
CHESHIRE, CT 06410

INSIDER THREATS ARE GETTING MORE DANGEROUS! HERE'S HOW TO STOP THEM

One of the most difficult types of attacks to detect are those performed by insiders.

An "insider" would be anyone that has legitimate access to your company network and data via a login or authorized connection.

Because insiders have authorized system access, they can bypass certain security defenses, including those designed to keep intruders out.

Since a logged-in user isn't seen as an intruder, those security protections aren't triggered.

A recent report by Ponemon Institute found that over the last two years:

- Insider attacks have increased by 44%
- The average cost of addressing insider threats has risen by 34%

4 Types of Insider Threats

- Malicious/Disgruntled Employee
- Careless/Negligent Employee
- 3rd Party with Access to Your Systems
- Hacker That Compromises a Password

Ways to Mitigate Insider Threats

Thorough Background Checks

When hiring new employees make sure you do a thorough background check.

Malicious insiders will typically have red flags in their work history.

You want to do the same with any vendors or contractors that will have access to your systems.

Endpoint Device Solutions

Mobile devices now make up about 60% of the endpoints in a company. But many businesses aren't using a solution to manage device access to resources.

Put an endpoint management solution in place to monitor device access. You can also use this to safelist devices and block unauthorized devices by default.

Multi-factor Authentication & Password Security

One of the best ways to fight credential theft is through multi-factor authentication.

Hackers have a hard time getting past the 2nd factor.

They rarely have access to a person's mobile device or FIDO security key.

Employee Data Security Training

Training can help you mitigate the risk of a breach through carelessness.

Train employees on proper data handling and security policies governing sensitive information.

Network Monitoring

Use AI-enabled threat monitoring.

This allows you to detect strange behaviors as soon as they happen.

For example, someone downloading a large number of files.

Or someone logging in from outside the country.

MEET MICROSOFT VIVA SALES

Data entry can be a real drag for salespeople. The time they spend on administrative tasks is time away from customer interactions. But that data is vital.

It's important to capture customer orders, quotes, needs, and more. Lead and sales reporting help sales managers know where to direct their attention. Analytics also help drive more efficient ways of closing the deal.

Microsoft has taken up the mantle of this challenge. It is about to launch a new digital experience for sales teams. Microsoft Viva Sales is part of the "Viva" line of applications. It is a "CRM helper" application, but not designed to replace your current CRM.

Microsoft Viva Sales Basics

- Eliminate Forms
- Powerful Data Leveraging
- AI-Driven Help
- Interconnected Interface

Tag to Capture Sales Interactions

Salespeople can use the familiar tagging function to capture data from another M365 application for a prospect or customer.

Collaborate

Viva Sales makes it easier than ever to collaborate with your team.

Call Summaries & Integrated Data

Viva Sales brings all that customer engagement data together into a single view.

This allows the salesperson to see call summaries and capture call action items.

Download & Customize

Download lead and customer lists. Customize the application per the organization's needs.

Take Advantage of Microsoft Viva Automation

Microsoft built the Viva suite of digital experience apps for productivity. These apps help employees find information faster, feel more connected, and work more productively.

SECURITY TIPS FOR ONLINE HOLIDAY SHOPPING

The holiday shopping season is taking off. This means that scammers have also revved up their engines. They're primed and ready to take advantage of all those online transactions.

Here are some of the most critical safety tips to improve your online holiday shopping.

- Check for Device Updates Before You Shop
- Don't Go to Websites from Email Links
- Use a Wallet App Where Possible
- Remove Any Saved Payment Cards After Checking Out
- Make Sure the Site Uses HTTPS (Emphasis on "S")
- Double Check the Site URL
- Never Shop Online When on Public Wi-Fi
- Be On High Alert for Brand Impersonation Emails & Texts
- Enable Banking Alerts & Check Your Account

CHECKLIST FOR OFFBOARDING EMPLOYEES

When an employee leaves a company, there is a process that needs to happen.

This is the process of "decoupling" the employee from the company's technology assets.

This digital offboarding is vital to cybersecurity.

- Knowledge Transfer
- Address Social Media Connections to the Company
- Identify All Apps & Logins the Person Has Been Using for Work
- Change Email Password
- Change Employee Passwords for Cloud Business Apps
- Recover Any Company Devices
- Recover Data on Employee Personal Devices
- Transfer Data Ownership & Close Employee Accounts
- Revoke Access by Employee's Devices to Your Apps and Network
- Change Any Building Digital Passcodes

WHAT ARE THE MOST HELPFUL VOIP FEATURES FOR SMALL BUSINESSES?

During the pandemic, VoIP and video conferencing have skyrocketed by over 210% due to the move to remote work and hybrid offices. Sixty-seven percent of surveyed companies say switching to VoIP helps improves call handling.

The technology is much cheaper to use than a traditional landline-based system. Calling plans are also often less expensive, and a company can add new numbers for very little cost.

VoIP has several helpful features for small businesses, but *what are the best features to drive efficiency, productivity, and positive caller experience?*

- Automated Attendant
- Find Me/Follow Me
- Hold Music
- Voicemail Transcription to Email
- Ring Groups
- Call Reporting
- Local Support

TECHNOLOGY TRIVIA

Each month you have a chance to win a $50 Amazon Gift Voucher by being the first person to email us with the answer to our Technology Trivia Question of the Month!

The question this month is:

What was the first book sold on Amazon?

The first person to email me at info@bluecastleit.com with the correct answer gets a $50 Amazon Gift Card!