JANUARY 2023

TECH TALK

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

INSIDE THIS ISSUE:

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing Technology!

- **Scott Magee**
Managing Director

WHAT'S CHANGING IN THE CYBERSECURITY INSURANCE MARKET?

Cybersecurity insurance is still a pretty new concept for many SMBs. It was initially introduced in the 1990s to provide coverage for large enterprises. It covered things like data processing errors and online media.

Since that time, the policies for this type of liability coverage have changed. Today's cyber insurance policies cover the typical costs of a data breach. Including remediating a malware infection or compromised account.

Cybersecurity insurance policies will cover the costs for things like:

- Recovering compromised data
- Repairing computer systems
- Notifying customers about a data breach
- Providing personal identity monitoring
- IT forensics to investigate the breach
- Legal expenses
- Ransomware payments

The increase in online danger and rising costs of a breach have led to changes in this type of insurance.

No one is safe. Even small businesses find they are targets. They often have more to lose than larger enterprises as well.

The cybersecurity insurance industry is ever evolving. Businesses need to keep up with these trends to ensure they can stay protected.

Demand is Going Up

The average cost of a data breach is currently $4.35 million (global average).

In the U.S., it's more than double that, at $9.44 million. As these costs continue to balloon, so does the demand for cybersecurity insurance.

Companies of all types are realizing that cyber insurance is critical. It's as important as their business liability insurance.

With demand increasing, look for more availability of cybersecurity insurance.

Premiums are Increasing

With the increase in cyberattacks has come an increase in insurance payouts. Insurance companies are increasing premiums to keep up.

In 2021, cyber insurance premiums rose by a staggering 74%.

Insurance carriers aren't willing to lose money on cybersecurity policies.

Certain Coverages are Being Dropped

Certain types of coverage are getting more difficult to find. For example, some insurance carriers are dropping coverage for "nationstate" attacks. These are attacks that come from a government.

Many governments have ties to known hacking groups. So, a ransomware attack that hits consumers and businesses can very well be in this category.

In 2021, 21% of nation-state attacks targeted consumers, and 79% targeted enterprises. So, if you see that an insurance policy excludes these types of attacks, be very wary.

Another type of attack payout that is being dropped from some policies is ransomware.

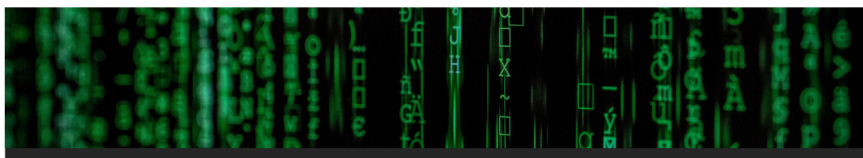
Insurance carriers are tired of unsecured clients relying on them to pay the ransom. So many are excluding ransomware payouts from policies. This puts a bigger burden on organizations.

It's Harder to Qualify

Just because you want cybersecurity insurance, doesn't mean you'll qualify for it. Qualifications are becoming stiffer. Insurance carriers aren't willing to take chances. Especially on companies with poor cyber hygiene.

Some of the factors that insurance carriers look at include:

- Network security
- Use of things like multi-factor authentication
- BYOD and device security policies
- Advanced threat protection
- Automated security processes
- Backup and recovery strategy
- Administrative access to systems
- Anti-phishing tactics
- Employee security training



Sentinel One - The next generation of protection

Today's security teams and businesses need flexible and robust prevention, detection, and response to secure every endpoint, no matter where they are in the world.

Sentinel One, who are both a cybersecurity research firm and software vendor, are aiming to revolutionize the world of Endpoint protection and antivirus by harnessing the power of Artificial Intelligence to detect and remediate threats before they even occur.

This unique software develops a timeline of attacks to allow security teams take control of a situation and resolve any threats that might come their way in a timely fashion.

Contact us now to find out how Sentinel One can help protect your business.

Cirrus IT Services

ALIGN YOUR TEAM TO COMPANY TARGETS WITH MICROSOFT VIVA GOALS

You often hear the words "digital transformation" and "collaboration." But what do they actually mean? What do they mean for the day-to-day of running your business?

Collaboration can't happen without shared goals. When departments are siloed and unconnected, priorities can conflict. People are doing their best but may not be moving in the same direction.

Digital transformation is simply the use of technology to better reach business goals. This encompasses moving from analog ways of doing things. Transitioning to tools that are more automated and connected.

Microsoft has been at the forefront of digital transformation and collaboration. Its Viva platform drives an improved employee experience. It does this by use of AI, automation, cloud connectivity, and more.

What is Viva Goals?

Viva Goals is one of the newest Viva applications from Microsoft.

It connects teams so they're moving toward a shared set of goals. Employees align, whether someone works in the accounting department or customer support.

Business leaders can look at Viva Goals as a way to solidify company objectives. They can then tie these objectives to meaningful targets for each department.

For example, say you have a corporate target to provide exceptional customer support. This goal by itself is generic. It doesn't connect to what teams need to do to make it happen.

In Viva Goals, that target can have directives for various teams. Such as customer support reducing ticket resolution by 8 hours. This brings goals to a meaningful level and allows organizations to track progress.

Here are the key value-adds of using Viva Goals.

Aligns Your Team to the Same Goals

Viva Goals puts company goals and targets in a tangible form. There is a definition of success for teams and individuals. Work outcomes are directly connected to company-wide objectives.

Maintains Focus on Goals

Viva connects to other M365 apps, making it easier to gather data insights. These insights help leaders more easily see goal progress.

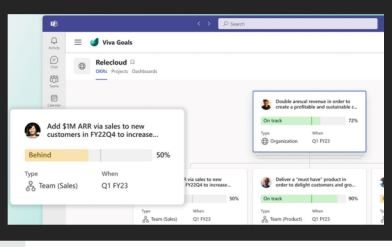
Employees stay focused on goals. This is because goals connect to their daily work targets.

Rather than being something they hear at a company event, goals get infused into the workflow.

Integration with Teams & M365

The integration with Teams keeps goals front and center. Employees get recognized for meeting targets and helping the company achieve its goals.

This keeps everyone engaged and moving together.



WHAT CYBERSECURITY ATTACK TRENDS SHOULD YOU WATCH OUT FOR IN 2023?

Cybersecurity risks are getting worse. Attacks continue to get more sophisticated. They are also often perpetrated by large criminal organizations. These criminal groups treat these attacks like a business.

To protect your business in the coming year, it's important to watch the attack trends. We've pulled out the security crystal ball to tell you what to watch out for.

Attacks on 5G Devices

Hackers are looking to take advantage of the 5G hardware used for routers, mobile devices, and PCs. Any time you have a new technology like this, it's bound to have some code vulnerabilities.

One-time Password (OTP) Bypass

This alarming new trend is designed to get past one of the best forms of account security – Multi-factor authentication. Some ways this is done include:

- Reusing a token
- Sharing unused tokens
- Leaked token
- Password reset function

Attacks Surrounding World Events

People need to be especially mindful of phishing scams surrounding global crisis events.

Smishing & Mobile Device Attacks

Mobile devices go with us just about everywhere. Look for more mobile device-based attacks, including SMS-based phishing ("smishing").

Elevated Phishing Using AI & Machine Learning

Criminal groups elevate today's phishing using AI and machine learning. Not only will it look identical to a real brand's emails, but it will also come personalized.

7 VOIP SETUP TIPS FOR A MORE PRODUCTIVE OFFICE

Companies that don't set up their VoIP system efficiently, can experience issues.

This includes things like dropped calls, low bandwidth, and features left unused.

If you've been struggling to make your cloud phone system more efficient, check out these tips below. They provide setup best practices for VoIP.

1. Check Network Capabilities
2. Prioritize Your VoIP Software Using QoS Rules
3. Provide Quality Headsets for Your Team
4. Set Up Departments & Ring Groups
5. Create Your Company Directory
6. Have Employees Set Up Their Voicemail & VM to Email
7. Train Your Team on the Call Handling Process

5 WAYS TO BALANCE USER PRODUCTIVITY WITH SOLID AUTHENTICATION PROTOCOLS

One constant struggle in offices is the balance between productivity and security. If you give users too much freedom in your network, risk increases. But add too many security gates, and productivity can dwindle.

There are ways to have both secure and productive users. It simply takes adopting some solutions that can help. These are tools that improve authentication security. But do it in a way that keeps user convenience in mind.

- Use Contextual Authentication Rules
- Install a Single Sign-on (SSO) Solution
- Recognize Devices
- Use Role-based Authentication
- Consider Adding Biometrics

DON'T SET YOURSELF UP TO FAIL: TIPS FOR SAFER HOME SECURITY SETUPS

From Ring doorbell cams to entire home security systems, watching your front door from afar has never been so easy. These security solutions also provide peace of mind at a wallet-friendly cost.

But don't let the ease of setup fool you. Home security devices can open your family up to risks if you don't take precautions.

There are many horror stories online about hacked video cameras. Don't let that scare you off. You can properly secure a home video camera system to ensure it's not breached. Here are some tips:

- Make Sure Your Router is Secure
- Change the Default Username & Password
- Ensure the System Uses SSL/TLS Or Other Encryption
- Keep the Software Updated
- Consider Access Levels for Multiple Users
- Enable Camera Security Features
- Make Sure Your Mobile Device is Secure

TECHNOLOGY TRIVIA TIME

Each month you have a chance to win an Amazon Gift Card! Our December competition winner (randomly selected from correct entries) was:
Kelly Lord
CAPLL Ltd.

The question this month is:

Why does Google rent out goats?

Email us at hello@cirrusits.co.uk with the correct answer by 15th January 2023 for your chance to win! Good Luck!