December 2023

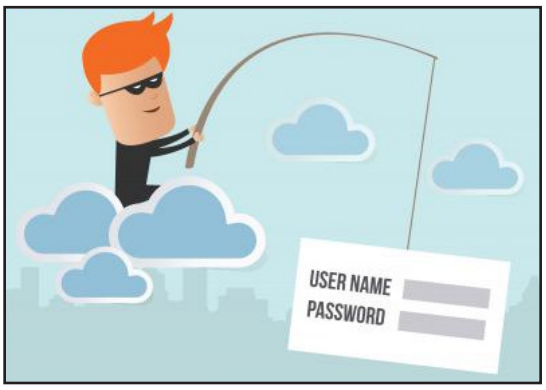
TechTidbit.com

brought to you by Tech Experts

Hackers Don't Take Holidays - Ransomware Is On The Rise

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Studies have shown up to a 70% increase in attempted ransomware attacks during the holiday season. That's what's happening in the cyber world right now.



Although we may be planning for a restful holiday ahead, full of delicious food and time with loved ones, hackers are not. Their ongoing exploitation of vulnerabilities and ever-changing tactics requires you and your team to be as vigilant as ever.

Phishing attacks have reached record highs this year. Worryingly, in the third quarter of this year alone, phishing attacks skyrocketed by a staggering 173%, compared to the previous three months.

And malware? It's not far behind, with a 110% increase over the same period.

Let's put this into perspective. Imagine you're on a quiet beach, enjoying the sun and the surf. Suddenly, the tide starts to rise rapidly. Before you know it, your picnic basket is floating away, and you're knee-deep in water.

According to a report, the 'phisherfolk' group were most active in August, casting out more than 207.3 million phishing emails. That's nearly double the amount in July. September wasn't much better, with 172.6 million phishing emails.

But who are these cyber criminals targeting? Old favorites Facebook and Microsoft continue to top the charts, with Facebook accounting for more phishing URLs than the next seven most spoofed brands combined. **Block Facebook on your network.**

So, what's the bottom line here? The attacks are coming from everywhere, and your business could be next.

Phishing attacks are like a rising tide, and if you're not careful, they can quickly sink your business. They target everyone - from tech giants to financial institutions, and even government agencies. The question is - are you prepared?

Take a moment to consider the authenticity of emails. Are they from a trusted source? Do they contain suspicious links? Are they asking for sensitive information?

Make sure your employees are aware of the risks. Encourage them to think twice before clicking on a link or downloading an attachment. After all, a moment's hesitation could save your business from a devastating cyber attack.

And don't forget about integrated email security solutions and phishing awareness training. They could be the things that best help you prevent an attack.

So, as the tide of phishing attacks continues to rise, remember – it's better to be safe than sorry.

If you need any further help or advice, get in touch.

But who are these cyber criminals targeting? Old favorites Facebook and Microsoft continue to top the charts, with Facebook accounting for more phishing URLs than the next seven most spoofed brands combined.

Should Your Business Follow Google's Security Lead?

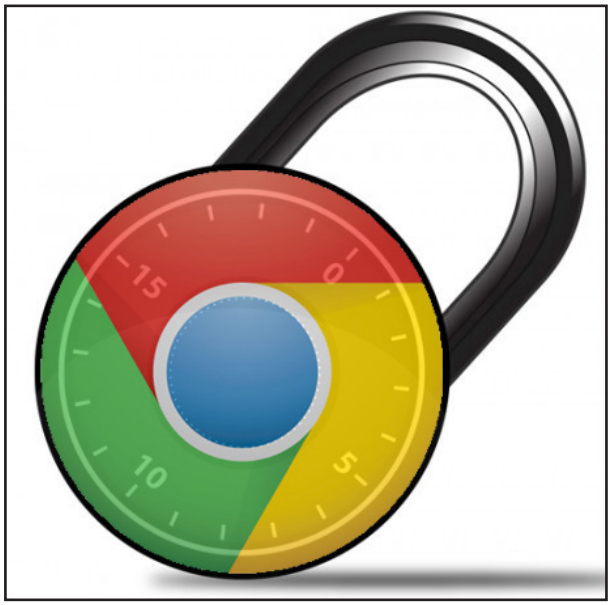
"Research shows that insider threats account for 62% of all security breaches. These insiders – disgruntled employees, careless staff, or malicious actors – often have legitimate access rights, intimate knowledge of the system, and can bypass traditional security checks."

Google has introduced a new security strategy – but is it right for your business?

It has put some employees on a cyber diet, restricting their internet access to limit potential threats.

On the surface, it sounds like a smart move. Google's approach is like building a taller fence around your house to keep out burglars.

By reducing internet connectivity, they're effectively shrinking their digital footprint and making it harder for cyber criminals to find a way in.



But is it foolproof?

Well, not exactly.

While this strategy does limit external threats, it doesn't entirely eliminate the risk.

Think of it this way: you've built a towering wall around your house, but your teenager leaves the back gate open. Similarly, internal systems might remain connected to other devices that can access the internet, providing a potential entry point for cyber threats.

In other words, you can't just focus on keeping things out.

Yes, there are very real threats from external hackers using all sorts of techniques like phishing, zero-day attacks, and malware. But the security industry often overlooks significant threats from within the perimeter.

Research shows that insider threats account for 62% of all security breaches. These insiders – disgruntled employees, careless staff, or malicious actors – often have legitimate access rights, intimate knowledge of the system, and can bypass traditional security checks. It's like having a burglar who knows where you hide your spare key.

So, what's the takeaway?

While Google's strategy has its merits, it's not a one-size-fits-all solution. Just as you wouldn't wear shoes that are too big, your business needs a cyber security strategy tailored to fit its unique requirements. A robust cyber security strategy should focus on both external and internal threats and have measures in place to mitigate risks from all angles.

Our advice? Instead of simply following in Google's footsteps, consider your own business's needs and vulnerabilities. And of course, if you need help with that, get in touch.

We Love Referrals!

The greatest gift anyone can give us is a referral to your friends and business colleagues. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll give them their free first month of service (for being a friend of yours) AND we'll give you a $250 Amazon Gift Card.

Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

How To Organize Your Cybersecurity Strategy Into Left And Right Of Boom

In the pulsating digital landscape, every click and keystroke echoes through cyberspace. The battle for data security rages on.

Businesses stand as both guardians and targets. Unseen adversaries covet their digital assets. Businesses must arm themselves with a sophisticated arsenal of cybersecurity strategies.

On one side, the vigilant guards of prevention (Left of Boom). On the other, the resilient bulwarks of recovery (Right of Boom). Together, these strategies form the linchpin of a comprehensive defense. They help ensure that businesses can repel attacks. And also rise stronger from the ashes if breached.

What Do "Left of Boom" and "Right of Boom" Mean?

In the realm of cybersecurity, "Left of Boom" and "Right of Boom" are strategic terms. They delineate the proactive and reactive approaches to dealing with cyber threats.

"Left of Boom" refers to preemptive measures and preventative strategies. These are things implemented to safeguard against potential security breaches. It encompasses actions aimed at preventing cyber incidents before they occur.

"Right of Boom" pertains to the post-breach recovery strategies. Companies use these after a security incident has taken place. This phase involves activities like incident response planning and data backup.

Together, these terms form a comprehensive cybersecurity strategy. They cover both prevention and recovery aspects.

Left of Boom: Prevention Strategies

User education and awareness: One of the foundational elements of Left of Boom is employee cybersecurity education. Regular training sessions can empower staff.

Robust access control and authentication: Access control tactics include:

- Least privilege access
- Multifactor authentication (MFA)
- Contextual access
- Single Sign-on (SSO) solutions

Regular software updates and patch management: Left of Boom strategies include ensuring all software is regularly updated.

Network security and firewalls: Firewalls act as the first line of defense against external threats. Install robust firewalls and intrusion detection/prevention systems that alert quickly when a breach is in progress.

Regular security audits and vulnerability assessments: Conduct regular security audits and vulnerability assessments. This helps to identify potential weaknesses in your systems.

Right of Boom: Recovery Strategies

Incident response plan: Having a well-defined incident response plan in place is crucial.

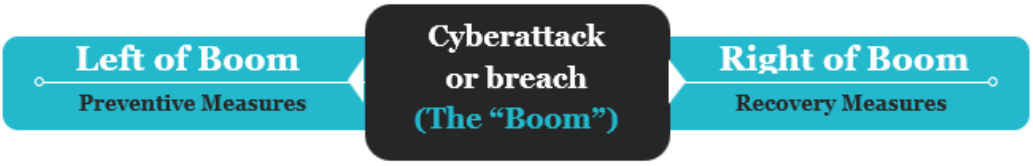
It should include things like:

- Communication protocols
- Containment procedures
- Steps for recovery
- IT contact numbers

Data backup and disaster recovery: Regularly backing up data is a vital component of Right of Boom. Another critical component is having a robust disaster recovery plan.

Forensic analysis and learning: After a security breach, conduct a thorough forensic analysis. It's essential to understand the nature of the attack. As well as the extent of the damage, and the vulnerabilities exploited.

Legal and regulatory compliance: Navigating the legal and regulatory landscape after a security breach is important.



"In the realm of cybersecurity, 'Left of Boom' and 'Right of Boom' are strategic terms. They delineate the proactive and reactive approaches to dealing with cyber threats."

Contact Information

Tech Experts Support Team
(734) 240-0200
support@MyTechExperts.com

Main Office
(734) 457-5000
info@MyTechExperts.com

Sales Inquiries
(888) 457-5001
sales@MyTechExperts.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Cyber-Compliance Is Serious Business

If you've never experienced a cyberattack, you might not think it's such a big deal.

Especially if you work in management, you're so busy focusing on the so-called squeaky wheels of every day; does it really matter if you keep up with the intricacies of modern cybersecurity compliance protocol? YES!

Increased digitization across the globe plus ever-advancing cyber threats equals a constantly evolving market, and legislation that scrambles to keep up.

Why Reporting Matters in a Data Breach

Have you ever experienced a cyberattack, either aimed at you or leveled at your organization? If so, then you might already know how important it is to report the breach - and we don't just mean to your direct managers or the police!

When a data breach happens, you are often beholden to laws detailing what, how fast and to whom you must disclose. For example, financial institutions have to notify the Federal Trade Commission within thirty days.

You typically have to disclose the breach to anyone affected too, depending on what information was stolen. Where do you work? Do you know the laws set upon your industry and role?

So not only does cyber-compliance affect your ability to protect yourself and your customers from a data breach, but that hack will affect customers' trust in your ability to keep their personal and financial information safe.

There are also legal concerns to think about. Lawsuits can cost millions between legal fees, penalties, profit losses and disruptions to the daily workflow.

Consider that the average company spends $10K per employee on cyber-compliance, and you see why maintaining compliance saves millions – about half of what you'd spend if you let vulnerabilities lay rampantly unpatched.

Maintaining compliance isn't just smart; it's necessary. To foster good relationships with your customers and shareholders, and avoid fines and breaches, companies must maintain a compliant cybersecurity structure.

These regulations change over time but do so to keep up with the latest tricks up cybercriminals' sleeves.

Our IT services include compliance as part of our all-in-one package to reduce excess labor on your end. We'll stay up to date on changing regulations so you stay cyber-compliant!

Reporting is one of many important regulations that make you more cyber-secure. Think about it: If your bank accounts, or health records, or mailing information got leaked, wouldn't you want to know?

It's not just about preferences, though. Data privacy is a right in many countries across the globe. More and more, people and legislation are all pushing for better data privacy protections.

How can we keep our accounts and data private if we don't know when a breach has occurred? If you don't know YOUR reporting requirements, now is the time to find out! Give us a call.