IMAGINE IT

The Q2 2023 State of Cybersecurity

imagineiti.com

9 critical questions to ask your IT Director or MSP

Many executives assume their IT Director or MSP has it covered. That incorrect assumption costs businesses billions of dollars every year.

In previous articles I discussed that the cybersecurity strategy starts in the boardroom. The board does not need to define a tactical strategy, but DOES need to manage risk and fully understand how the org addresses it.

Here's a list of questions to ask those responsible for maintaining org security...

- Where are we most at risk? Note: This should be quite a few areas, else probe more deeply.
- Do we follow a nationally recognized framework, like NIST CSF? Show me.
- Does a 3rd party perform an annual Vulnerability Assessment? Show me the results.
- Do we have a 2-year gap remediation roadmap? Show me.
- Is our backup system immutable and MFA protected? Show me.
- Can we take action against critical security alerts 24/7? Show me how.
- Do we outsource Threat Hunting? Show me a report.
- When was the last time the Incident Response and Disaster Recovery Plans were tested? Show me the results.
- Do we score our cybersecurity posture against national standards? Cyber insurance? Compliance? Show me.

Notice these questions require PROOF. Cybersecurity is just too critical to your business to take someone's word for it, even if it is someone you trust.

If you don't get proof, consider engaging with an MSP with a high cybersecurity acumen. Ask THEM how they would answer those questions, and have them provide evidence.

What you can do to protect your business

Deploy Additional Email Protection

Most security threats to your business arrive in an email, including ransomware. Yes, security awareness training is critical, but so is blocking malicious messages BEFORE they arrive in mailboxes.

The Solution

Microsoft provides an additional subscription called “Microsoft Defender for Office 365” that addresses this issue. Here are the relevant features...

- Scans attachments and links for malicious content BEFORE the message arrives to the user.
- Scans SharePoint and OneDrive files for malicious links.
- Scans Teams content for malicious attachments and links.

Defender scans each time an attachment or link is accessed, thereby assuring it is still safe. The scanning process happens in seconds and does not slow down the user.

Many businesses already subscribe. If you are unsure, please engage with your MSP.

What’s around the corner?

Impending National Privacy Laws

The introduction of national privacy laws in the United States will have a significant impact on small businesses. While the laws will provide a uniform standard for the protection of personal data, they will also require small businesses to comply with new regulations and potentially invest in new technology and resources.

One of the main ways in which national privacy laws will impact small businesses is through increased compliance costs. Small businesses may need to invest in new technology, software, and personnel to comply with the new regulations. This can be especially burdensome for smaller businesses with limited resources.

Another way in which national privacy laws will impact small businesses is through increased liability for data breaches. Under the new laws, small businesses may face greater penalties and legal liabilities if they fail to adequately protect personal data. This could lead to increased costs and potential lawsuits.

However, national privacy laws may also provide some benefits to small businesses. For example, the laws could help to level the playing field for smaller businesses by creating a uniform standard for data protection. This could help to build trust with consumers and increase competition.

Overall, the impact of national privacy laws on small businesses will depend on the specific regulations and requirements established. While the laws may impose some additional costs and burdens, they could also provide some benefits in terms of increased consumer trust and competition. As such, small businesses should stay informed about the development of national privacy laws and take steps to prepare for potential compliance requirements.

Peter's Insight on National Privacy Laws:

Currently, only a few states have privacy laws. However, there is momentum at the national level driving bipartisan congressional legislation. It will likely get passed in the next year or so. Once that happens, there is typically a 2-3 year deadline set for businesses to comply.

Security pro-tip of the quarter

Gift Card Scams

Gift card phishing scams are a form of scam where a cybercriminal poses as a CEO or other high-level executive of a company and sends a message to an employee asking them to purchase gift cards or transfer money. Here are some examples of gift card phishing scams:

- CEO impersonation: The scammer sends an email or text to an employee that appears to be from the CEO, asking them to purchase gift cards or transfer money urgently. The email may include a sense of urgency or pressure the employee to act quickly.
- Vendor impersonation: The scammer sends an email to an employee that appears to be from a vendor or supplier, asking them to purchase gift cards as payment for services or products. The email may include a sense of urgency or a deadline for payment.
- Fake invoices: The scammer sends an email to an employee that appears to be a legitimate invoice, requesting payment via gift card. The email may include a request for the gift card information to be sent via email or phone.

- Payroll scams: The scammer sends an email to an employee that appears to be from the CEO, requesting personal information, including gift card information, to process their payroll or bonus.
- Executive assistant scams: The scammer sends an email to an employee that appears to be from an executive assistant or other high-level executive, requesting gift cards to be purchased for the CEO or other executives as a gift.

To avoid falling victim to gift card phishing scams, employees should be cautious and verify any request for gift cards or money transfers through a different means of communication, such as a phone call or face-to-face conversation. Companies should also establish clear policies and procedures for money transfers and gift card purchases, and educate employees on how to recognize and report potential scams.

Peter's Insight on Gift Card Scams:

DOZENS of our customers have fallen victim. There is something about an email from the CEO (or similar role) that makes users just nervous enough to miss the red flags. Recurring security awareness training is critical.

Conclusion

If one of your roles is to manage risk, make sure you fully understand where the risks are and how they are being addressed. Don't assume someone you trust has it covered.