IMAGINE IT

The Q2 2022 State of Cybersecurity

imagineiti.com

The Competitive Advantage of a Strong Cybersecurity Posture

There are many good reasons to take cybersecurity seriously...

- Exposure of confidential information, trade secrets and intellectual property
- Failed compliance obligations
- Business operations downtime
- Damaged reputation / company morale
- Cyber Insurance policy canceled or significant premium increase
- Loss of revenue/customers/donors
- Reduction in business valuation
- ...and more

Would you consider adding to that list that a strong cybersecurity posture can be a competitive advantage? You sure can! Here are two examples we have seen firsthand...

WIN	LOSS
We have a customer with a strong posture. One of their competitors had a breach, and our customer was able to prove a strong posture and acquire many of the competitor's clients.	We have a customer that was trying to obtain a large enterprise client. Enterprise orgs typically require vendors to have a strong cybersecurity posture. This customer did not and was rejected during the security audit. Silver lining... this customer can now prove a strong posture, and recently obtained an enterprise client due to it.

So as you can see, having a strong cybersecurity posture can have a huge impact on your business.

What You Can Do To Protect Your Org

Dark Web Monitoring

When users and companies get breached, it is very common for the attackers to post login credentials and stolen data on the Dark Web - either for sale, or as a lever to get paid a ransom, or to just embarrass.

Most of the time the victim is unaware and might not even know they have been victimized.

This is where “Dark Web Monitoring” becomes very useful. Any time information is added to the Dark Web about your org, an alert is generated for IT staff to review. This allows IT staff to alert the user and take action...

- Change passwords, potentially in many places
- Scan for viruses
- Look for evidence of data exfiltration

Without Dark Web Monitoring an org may never know an incident has occurred.

What's Around The Corner?

Local Administrators Lockdown

How is it that malware successfully installs on a computer, even when antivirus software is running?

If the antivirus software does not detect the malware, the next line of defense is whether or not the user is allowed to install software...

- If yes, the malware successfully installs.
- If no, the malware is potentially blocked.

Most computer users are "Local Administrators" of their computers, and therefore can install applications and make settings changes. If a user is not a Local Administrator, they would need to engage with IT support every time they want to install software, a printer, or even a browser plug-in.

Allowing users to be Local Administrators also allows them to install software that is not approved, which of course includes malware.

That's the dilemma... lock it down and cause occasional delays or leave it vulnerable and allow the user to do what they want timely.

What if we could solve this dilemma – lock it down AND allow timely and approved installations? We can! Imagine IT is currently rolling out a solution called "AutoElevate".

AutoElevate allows users to be removed from the Local Administrators group (locked down), and provides an automated support desk notification when a user is requesting to perform an Administer task (like install software). The technician can then quickly analyze the request to make sure it is safe/allowed, then push a button to approve the install. Pretty simple!

Peter's Insight

One of the most basic cybersecurity best practices is to remove users from Local Administrator permissions. Logistically this has been a problem, but AutoElevate will now allow Imagine IT to enforce this very basic setting with very little impact to the users.

Security pro-tip of the quarter

Layers of Security

Defense in depth… Defense in layers… In football the "safety" backs up the "cornerbacks".

This is a basic tenant of a strong cybersecurity strategy. Without layers, each security defense mechanism will be left to fight alone. What if malware gets past the antivirus software? You will wish you had another layer (or two) to protect your data.

Here is a great example of "layered security" …

- The user is not a Local Administrator
- Malware scanning is performed on email attachments and links
- Malware scanning is performed at the firewall
- Malware scanning is performed on the computer
- Malware scanning is performed on each website URL visit
- Threat Hunting investigates suspicious activity

The Imagine IT Security Shield is a "deep-layered" strategy to protect your users and data. The Shield…

- Starts with an "identify" process to address the gaps.
- Deploys layers of "protection" and layers of "detection"
- Is backed up by a rock-solid Incident Response Process and immutable Backup & Recovery systems

With all those layers it will be extremely tough for hackers to successfully execute their mission.

Conclusion

When making strategic cybersecurity decisions, be mindful of the business impacts of a breach, and how you can spin a strong cybersecurity posture in your favor.