IMAGINE IT

The Q3 2021 State of Cybersecurity

imagineiti.com

In the previous quarterly update, I referenced "hacker feeding frenzy" and how the speed of developing attacks against vulnerabilities has increased significantly. Which brings us to my first topic...

The frequency of zero-day vulnerabilities

Vulnerabilities are security holes in devices or software. If the vulnerability is exploited by attackers BEFORE a patch is released, it is known as a "Zero-Day" vulnerability. Then it becomes a race to create a patch and publish mitigations to block the attack vector until a patch is released.

"Zero-Day's" are dangerous because often hundreds or thousands of orgs become victims before the vulnerabilities are fixed. MSSP's and IT staff are now forced to address zero-day vulnerabilities every week, whereas up until recently we addressed these exposures only a few times per year. This is becoming a full-time job for some.

Why is this suddenly happening? Up until recently, entities had ample time to patch vulnerabilities before hackers figured out how to attack them. But now it only takes a couple days for the hacking community to share the attack process with each other on the Dark Web. Nation-states and organized hacking are now better and faster than the thousands of ethical hackers, leaving all of us at risk.

What you can do to protect your org

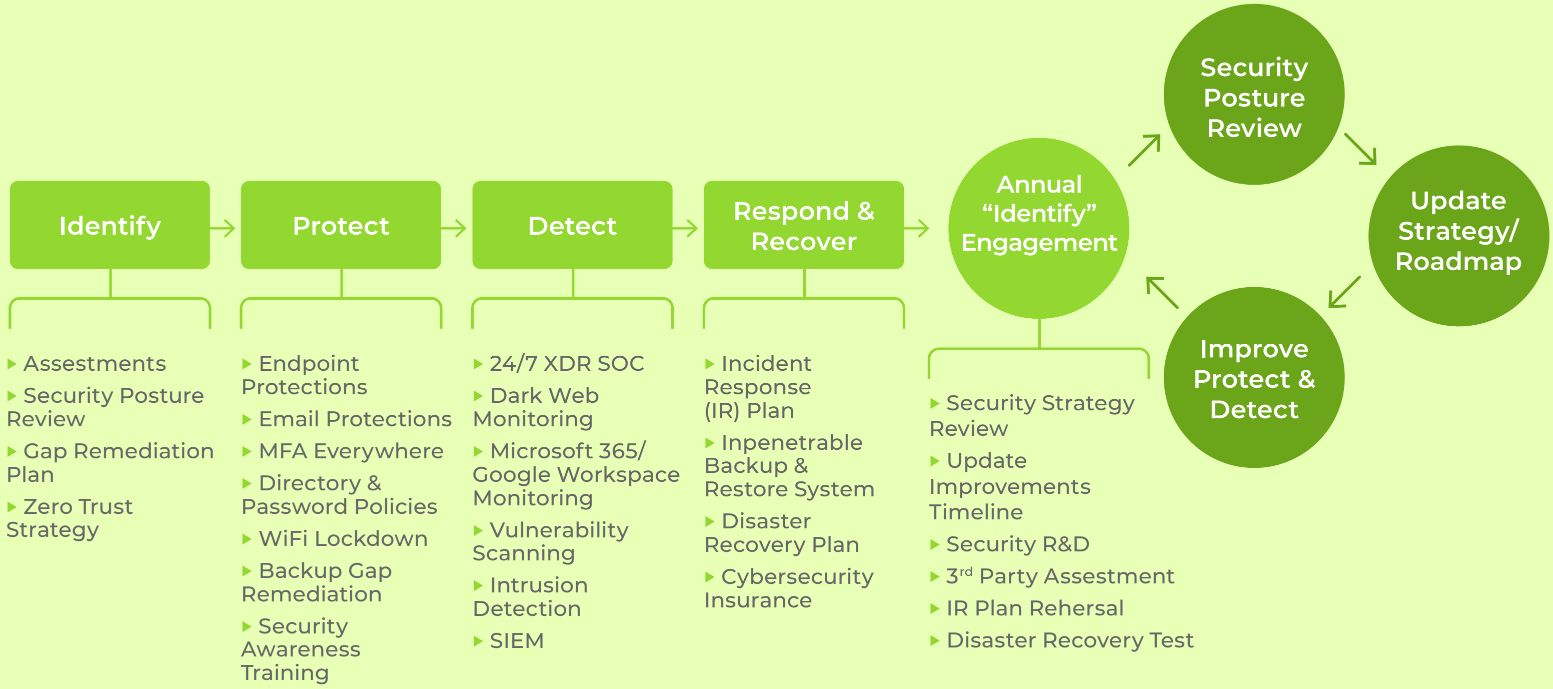
The first step is to acknowledge the risk exists and formulate a cybersecurity strategy. Unfortunately, all too many orgs still have their head in the sand.

In the previous quarterly update, I referenced the NIST Cybersecurity Framework (CSF). The CSF is a great model for securing your technologies and data.

At a high-level, your org needs to:

- Annually **identify** gaps and draft a remediation plan. This often starts with a 3rd Party Vulnerability Assessment. Since it would be a conflict of interest for Imagine IT to perform these assessments, we can recommend some trusted assessment entities.
- Deploy **Protection** technologies and policies to block attacks.
- Deploy **Detection** technologies to alert security personnel of a breach BEFORE it gets serious. In every successful attack that hits the news, it was not detected until too late.
- Develop an Incident **Response** Plan and perform an annual rehearsal. Keep in mind that an Incident Response Plan is worthless if you have not detected the breach (see previous bullet).
- Develop a Disaster **Recovery** Plan and test it annually. This is typically an exercise to fully test the backup system.

Below is a graphical example of the NIST Cybersecurity Framework. Those of you enrolled in our Security Shield program already benefit from this...



Identify → Protect → Detect → Respond & Recover → Annual "Identify" Engagement

Identify
- Assessments
- Security Posture Review
- Gap Remediation Plan
- Zero Trust Strategy

Protect
- Endpoint Protections
- Email Protections
- MFA Everywhere
- Directory & Password Policies
- WiFi Lockdown
- Backup Gap Remediation
- Security Awareness Training

Detect
- 24/7 XDR SOC
- Dark Web Monitoring
- Microsoft 365/ Google Workspace Monitoring
- Vulnerability Scanning
- Intrusion Detection
- SIEM

Respond & Recover
- Incident Response (IR) Plan
- Inpenetrable Backup & Restore System
- Disaster Recovery Plan
- Cybersecurity Insurance

Annual "Identify" Engagement
- Security Strategy Review
- Update Improvements Timeline
- Security R&D
- 3rd Party Assessment
- IR Plan Rehersal
- Disaster Recovery Test

Annual "Identify" Engagement → Security Posture Review → Update Strategy/ Roadmap → Improve Protect & Detect → Annual "Identify" Engagement

What’s Around The Corner?

One of the biggest threats to your systems is malicious website content that can expose your org to malware and ransomware. What are some of the threat vectors?

- **Email:** most attacks originate via malicious links or attachments in email.
- **Ads:** it has become very common for viruses to be embedded in website and social media platform ads.
- **Malicious Sites:** attackers often create new domains that look like legitimate ones, laced with viruses.
- **Compromised Legitimate Sites:** occasionally a legitimate site gets injected with malware, infecting visitors.

One way to protect against malicious website content is to deploy “Web DNS Filtering”. This technology verifies that websites are safe by scanning links at time of click, and scanning sites manually accessed via the web browser.

At the “office network” level, Imagine IT utilizes Web DNS Filtering to scan traffic when users are at the office. But what about remote work? Sometime soon our Security Shield customers will benefit from a “Roaming DNS Filtering Agent” that will scan traffic on business owned laptops when away from the office. Considering the state of remote work, this will be a valuable tool against malware.

Pete’s Insight

Even with Security Awareness Training, users will occasionally make a mistake. A proper cybersecurity strategy is “layered” and should protect the systems from many angles. For example, it is best practice to scan for malware on the endpoints, and via the firewall, and in email, and via Web DNS Content Filtering. If a virus gets past one of these protections, likely one of the other technologies will block it.

Security pro-tip of the quarter

Microsoft Defender Antivirus

Did you know that for Windows computers, the free antivirus (AV) is considered to be one of the best, even compared to enterprise next-gen antivirus? How did this come to be? Over the years Microsoft has put an enormous effort into becoming one of the top cybersecurity vendors in the world, and one of the first things they did was to strengthen their antivirus software. The cybersecurity community has recognized this, and many Managed Security Service Providers (like Imagine IT) are taking a hard look.

For personal/home computers, we encourage you to enable Microsoft Defender by clicking Start and typing **defender**, then selecting "Windows Security". Make sure all of the items are green, especially "Virus & threat protection" and "Firewall & network protection". Of note, if you subscribe to a paid antivirus solution, that brand of AV will likely disable Defender and you won't be able to enable it.

Conclusion

I have a homework assignment for you... Engage with a 3rd party to assess your cybersecurity posture before end of year, and then make a gap remediation plan. We can provide recommendations for trusted assessors.