IMAGINE IT

The Q4 2021 State of Cybersecurity

imagineiti.com

Who initially defines the cybersecurity strategy?

In our recent discussions with executives, it has become clear there is a large gap between the reality of the current threat landscape and executive-level perception of threats to their businesses. In effect, most businesses are bringing a knife to a gunfight. And to compound the problem, many executives are entirely disengaged from the high-level cybersecurity strategy and mistakenly assume "someone else" has it well-covered.

Kieran Norton, Deloitte Risk & Financial Advisory's infrastructure security solution leader and principal, Deloitte & Touche LLP, states...

"Strong executive and board-level oversight of and support for the cyber risk management program is a critical part of event preparedness. Leaders at the highest levels need to understand the crucial role they play by providing oversight, governance, and tone from the top."

A proper cybersecurity strategy secures the business assets, reputation, valuation, and shareholders, so the organization isn't blocked from achieving its objectives and/or shut down. Therefore, risk management and cybersecurity strategy are initially defined "in the boardroom" .... things like:

- Defining which systems can never be breached.
- Making sure the IT Director aligns the cybersecurity strategy with the business mission.
- Asking the IT Director to present the cybersecurity strategy to the board.

Bottom line, who is ultimately responsible if there is a serious breach? The Board and CEO/Director. If a breach causes serious mission issues or worse, the executives will be blamed.

Questions executives should ask the it director

(Don't assume the IT Director has it covered)...

- 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.
- Does the Incident Response (IR) Plan specifically address Ransomware? Show me.
- When was the last time the IR and Disaster Recovery Plans were tested? Show me the results.
- Is our backup system immutable, air-gapped, 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.

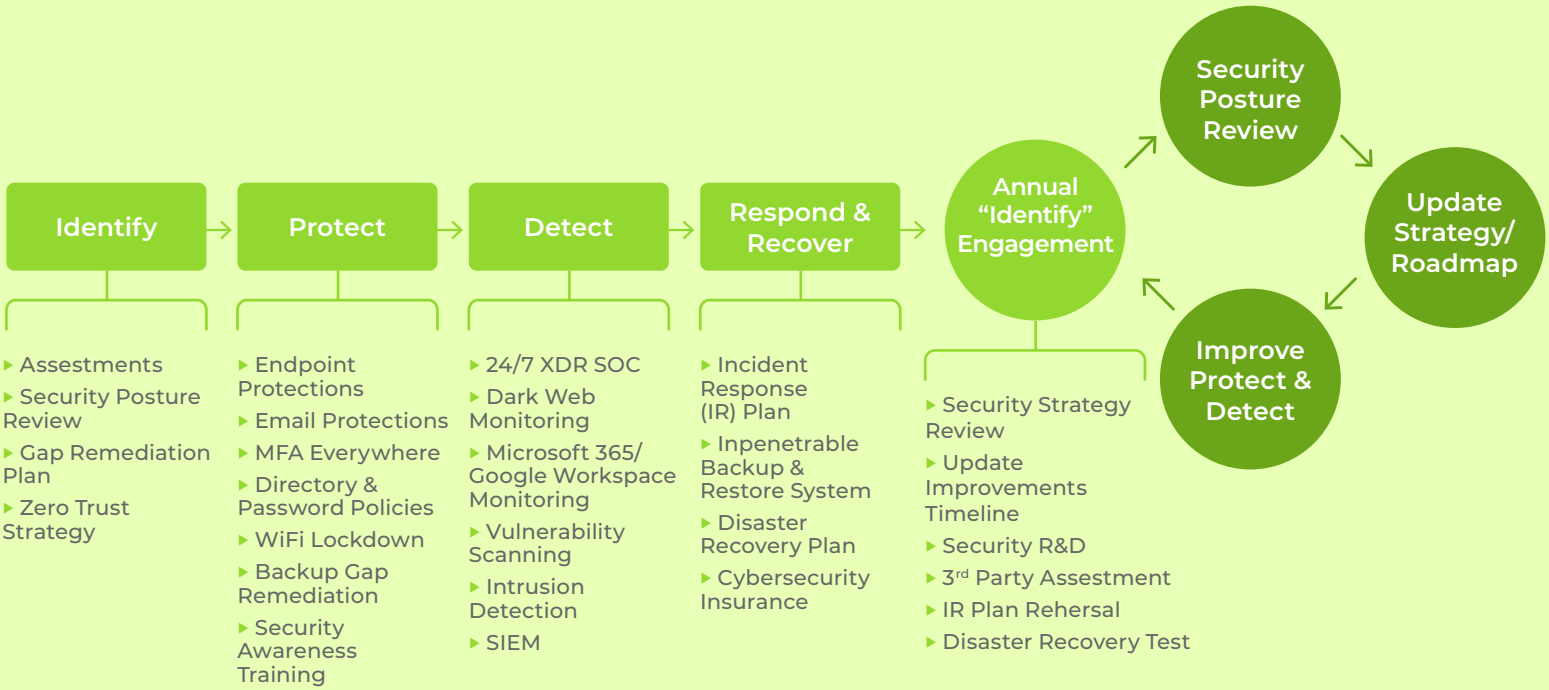
What you can do to protect your Org

Many organizations add 1-2 security protections per year. Long ago, this was OK. But today, the skill level of the attackers is exponentially greater, and organizations can no longer leave even the smallest vulnerabilities exposed.

The misguided "Security List" Approach vs. the best practice "Comprehensive" Approach

If you think of your cybersecurity posture in terms of your home, would you only lock "some" of the doors and windows now and lock a couple others in a few months? Of course not.

Below is a graphical example of the NIST Cybersecurity Framework, which is a "Comprehensive" approach. The goal is to complete at least 80% of the initiatives within 3 months – it's that critical. Those of you enrolled in our Security Shield program already benefit from this...



When an org takes the "Comprehensive" approach, it immediately and significantly reduces the risk of a serious breach and plans for "continual security posture improvement."

What's Around The Corner?

Users LOVE logging into multiple systems, multiple times per day, with different credentials AND Multi-Factor Authentication (MFA) – correct? Yeah, not so much.

This is where Single Sign-On (SSO) makes cybersecurity less intrusive. SSO consolidates the login process (and MFA) to multiple systems, reducing the number of logins per day. SSO can potentially integrate email, cloud apps, accounting, databases, and just about any modern system into a single login.

What does this potentially look like for a user? When they start their workday, they are prompted for a single username and password (plus MFA), allowing access to ALL integrated systems. Just one login – nice!

Pete's Insight

Does SSO create a security vulnerability with all the consolidation? Not when combined with "Conditional Access Policies" (CAP). CAP's define rules for each application and user/group. For example, email might prompt for login once per day, but highly sensitive data (like HR systems) might prompt 3 times per day. Step one is to identify what types of data are the most sensitive.

Security pro-tip of the quarter

Inbound Email Best Practices

Most breaches originate via email, so clearly, SPAM filtering is not enough to protect your org. Therefore, user security awareness is critical to limiting liability. Here are some user best practices...

- Set your email app to NOT display pictures:
  - ▸ The graphics can be malicious. And they also "phone-home" to advertisers.
- Hover over the email link to verify the URL address:
  - ▸ Verify the spelling of the URL is exactly as expected.
- NEVER click an unsubscribe link:
  - ▸ They could be fake and malicious.
  - ▸ Instead, send it to Junk Mail and empty it weekly or so.
- Instead of clicking a link, manually go to the website:
  - ▸ This is a little extra work but eliminates the chance of clicking malicious link.
- NEVER enable an MS-Office attachment "Editing" or "Macro" unless you 100% trust the attachment:
  - ▸ This is true even if you trust the sender. What if the sender has been compromised?

- Look for indicators of impersonation:
  - ▸ External sender banner displayed, yet the message is from a co-worker.
  - ▸ Wrong email address.
  - ▸ The timing or topic of the message seems strange.
- CALL the sender if suspicious:
  - ▸ NEVER reply to the message – it might be a hacker on the other end.
- Click the “Report Message” button if suspicious:
  - ▸ Some email systems have a button to report suspicious messages.

Users need to be constantly reminded of these best practices.

Conclusion

Do not assume the IT Director has cybersecurity covered. Ask questions and ask for proof – your business future may depend on it!