Challenges Facing Information Technology and Security Professionals

Mehran Basiratmand, PhD

eGroup + ENABLING TECHNOLOGIES

Challenges

- Responsible but lack the authority
  - Which end of the spectrum your IT security posture fall?
  - From Draconian to Charitable
- Decentralized nature of IT in various organizations
- Leadership Support
  - Please make it go away

eGroup + ENABLING TECHNOLOGIES

Challenges

- Lack of governance model (or champions)
  - IT Security Framework
  - Culture, appetite,
  - Addressing the regulatory requirements {HIPAA}
    - NIST, COBIT, Auditing, Logs, e-discovery & Reporting

eGroup + ENABLING TECHNOLOGIES

Challenges

- Patches coming 100 miles an hour
- Hybrid work schedule {Growing number of devices}
  - Personal devices
- Recertification of backup data in the cloud & on-site

eGroup + ENABLING TECHNOLOGIES

• BYOD Management

Image via Trend Micro – October 4th, 2022

Challenges

- Policy and Technology

eGroup + ENABLING TECHNOLOGIES

Image via Druva– October 4th, 2022 --- BYOD is a $350B business

Challenges

- **Great resignation & lack of adequate staffing given the salary structure in the public sector**
  - Unemployment for IT security staff
  - The cybersecurity occupation hit a 0% unemployment rate {Lifars publication}
- **Lack of consistent and adequate security training for end-user**

  (Security Education Training and Awareness SETA)

eGroup + ENABLING TECHNOLOGIES

Images from: DefenseWeb & Inc.com

Challenges

- **Most Security professionals are busy fighting fires vs serving as fire marshals to build a strong security posture**

eGroup + ENABLING TECHNOLOGIES

Images from: MN Fire Department, InfoSec Blog

Challenges

- **Cyber Security Insurance**
  - **Premiums increase**
    - **Cyber Security Insurance First Quarter 2022 by 37%**
- **Coverage has been reduced**
- **Expert underwriters have been hired**
- **Comprehensive questioner have been added to assess security pasture**

Image from: PTG

eGroup + ENABLING TECHNOLOGIES

NOW the GOOD Part

eGroup + ENABLING TECHNOLOGIES

Image from: ResearchGate

Recommendations

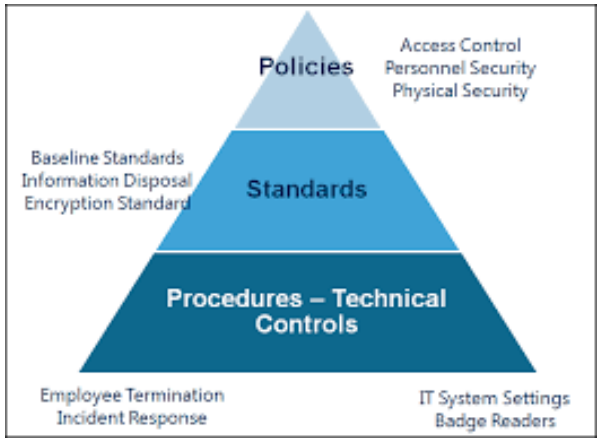
- Build a regular communication plan and build a trust with the clients
- Establish a governance model and seek input from stakeholders – we know sometimes it is like ….

Images from: tagg.com

eGroup + ENABLING TECHNOLOGIES

Recommendations

- Keep an up-to-date inventory of systems and services
  - Preferably with their versions
  - Keep this process consistent **so that you do not have to keep asking**
- You users should respect your views. Exemptions is not a norm

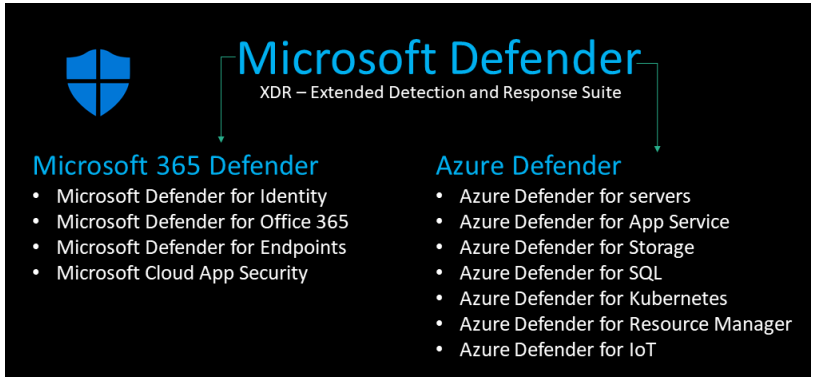


Images from: tagg.com

eGroup + ENABLING TECHNOLOGIES

Recommendations

- **Implement low-hanging fruits technologies that are generally available but may not have been implemented adequately**
  - MFA
  - Authentication Time to live
  - Improving employee's separation process to keep access up-to-date

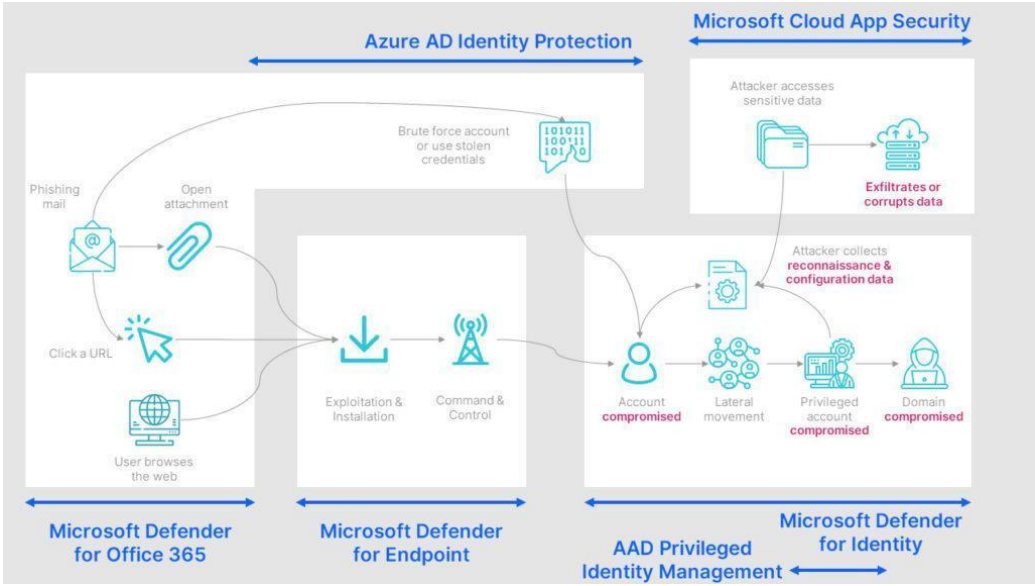


Images from: tagg.com

eGroup + ENABLING TECHNOLOGIES

Recommendations

- Take advantage of licenses you may already have in place.
  - DDM and MDM – Intune, Microsoft Defender for Endpoint, XDR



Images from: Microsoft

eGroup + ENABLING TECHNOLOGIES

Recommendations

- Microsoft Defender for Endpoint Plan 1 Now Included in M365 E3/A3/G3 Licenses
- Microsoft Defender for Office 365 Plan 2 is included in Office 365 E5, Office 365 A5, and Microsoft 365 G5

Everything you needed to know about Microsoft 1/3/5 licensing and were afraid to ask

https://www.infusedinnovations.com/blog/secure-modern-workplace/complete-office-365-and-microsoft-365-licensing-comparison

If you are already paying for another product as well as Microsoft, perhaps it would be good to review, compare and contrast your total cost of ownership – It could save $$$$

Images from: Microsoft

eGroup + ENABLING TECHNOLOGIES

Recommendations

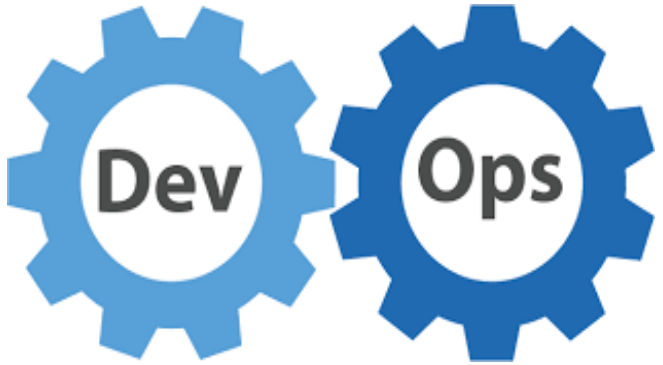
- **Seek augmented staffing for a time-limited & specific engagements**
  - There is an apprehension (hesitation) to get outside support for reasons such as {control, lack of knowledge transfer properly, airing dirty laundry or cost}
- **Virtual CISOs**

Images from: CyverGrape

eGroup + ENABLING TECHNOLOGIES

Recommendations

- Encourage sys admin to invest in a patch management software
  - Azure Update Management (Windows, Linux)
    - CentOS, Cost of Premier support (10 years), RedHat (https://endoflife.software/operating-systems/linux)
  - Microsoft Endpoint Configuration Manager
- DevOps patch management process for applications



Images from: fale.io & logolynx

eGroup + ENABLING TECHNOLOGIES

Recommendations

- Changing the model from decentralized to distributed
  - This is not to state sharing key to the kingdom or the crown jewels such as Azure Active Directory, but a shared governance model

Key to the Kingdom®

Images from: Keytothekigndom.com

eGroup + ENABLING TECHNOLOGIES

Recommendations

- Develop practical policies {outside of your regulatory requirements such as HIPAA) that are align with the organizational culture and appetite
  - **Us the three questions approach (Why, what is it going to do, how do we enforce it, measure it and use it)**

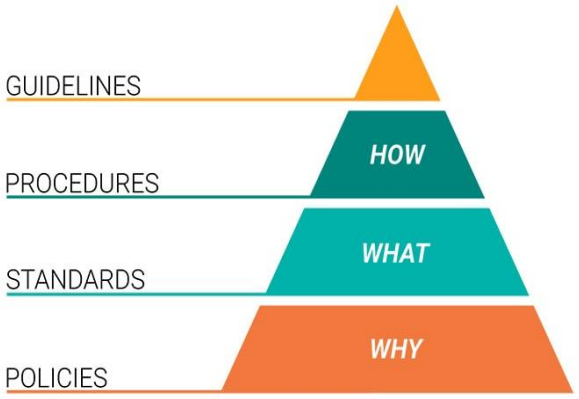


Image from: 7Sec.com

eGroup + ENABLING TECHNOLOGIES

Recommendations

- Engage in Tabletop Exercises and Simulation including Risk Assessment
  - Seek an outside entity to assist as you deem appropriate

Images from: NOAA

eGroup + ENABLING TECHNOLOGIES

Recommendations

- We generally do a great job of securing the perimeter, but it is far more difficult to secure personal devices. Need a coordinated effort at all levels
- Invest in a meaningful security training program

"Did you open an attachment from an unverified email?"

Images from: cyber security awareness

eGroup + ENABLING TECHNOLOGIES

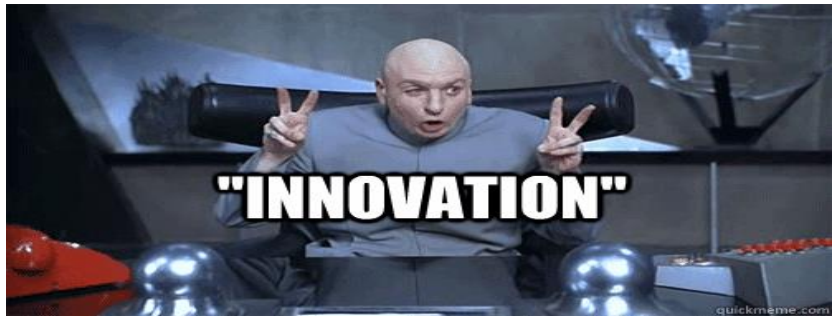
Recommendations

- Lowering your premiums
  - Review insurance questioner carefully
    - Backup, training & awareness, MFA on servers and switches, simulation, data encryption (in transit and at rest), access control, incident response, device management, policies
    - https://blog.goptg.com/20-cyber-insurance-questions (A generic version)
  - Work with a cyber insurance broker {Datastream, Gallegher, ProWriters, EPIC, AmWins}
    - https://www.reinsurancene.ws/top-20-us-cyber-insurance-companies/
    - https://www.esecurityplanet.com/products/cyber-insurance-companies/
  - **Work with a third-party technology company to validate your security posture**
- Do not share your coverage amount, since in a case of a ransomware attack, they will ask for that exact amount

eGroup + ENABLING TECHNOLOGIES

Spend time on security and technology innovation or encourage your organization to adopt this culture (3M 20% - in 70's- Google 2004)- if not realistic – try 10% or less of your time on R&D

DON'T BLAME TECHNOLOGY!



Images from: bcmblogs

eGroup + ENABLING TECHNOLOGIES

Questions?