The Most Common (root) causes of Cyber Breaches

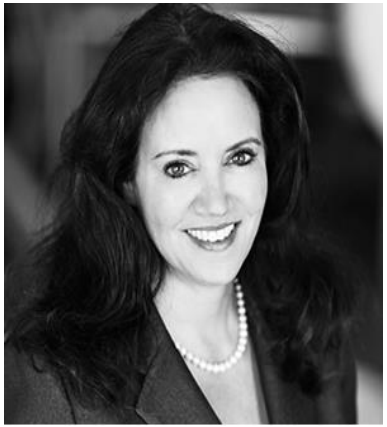
2022 Conference and Workshop

New York Metro Joint Cyber Security Coalition

2022 Conference and Workshop

Mary Frantz

Enterprise Knowledge Partners, LLC
Maryf@ekpartner.com



ENTERPRISE KNOWLEDGE PARTNERS, LLC

Because what you don't know, *can* hurt you

ENTERPRISE KNOWLEDGE PARTNERS, LLC

EKP. Because what you don't know CAN hurt you.

There is nothing more humbling than:

- ignored alerts and scans
- end-points you didn't lock down
- allowed or ignored transgressions by software engineers, executives, or third parties
- employee [sarcastic / painful] comments about breaking rules, poor security and compliance violations found in emails, chats and texts

Show up in the incident report and legal discovery - after a breach

Basics

ENTERPRISE KNOWLEDGE PARTNERS, LLC

EKP. Because what you don't know CAN hurt you.

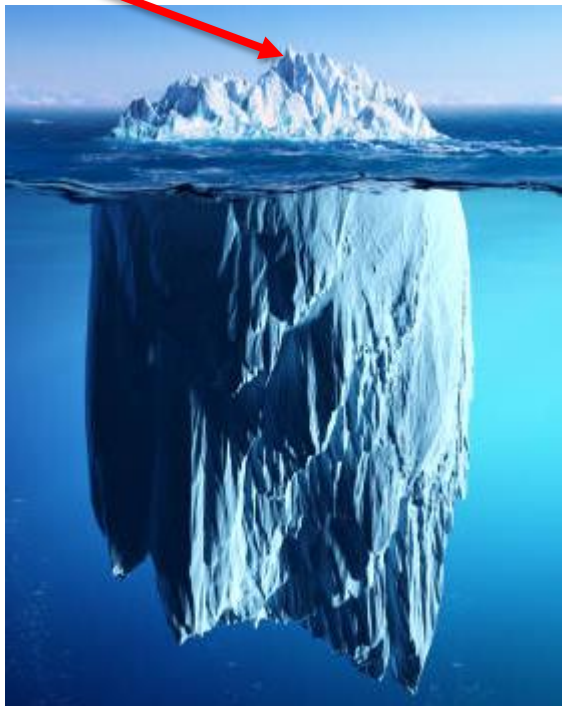
Most threat actors walk through the front door due to lack of basic security hygiene:

- Minimal or no asset management and identification
  - Lack of accurate and updated asset inventory; you can't protect what you don't know you have
- Lack of access management
  - Unsecured, unknown end-points
  - Systemically enforced access management based upon least privilege / separation of duties
- Lack of network segmentation
- Inadequate logging and monitoring
- Non-functional IR plan
  - Lack of meaningful IR testing

Cyber resilience and system efficiency go together – why is it so hard to do?

Company discovers this

Cyber incident
Investigation
discovery



Q3 2022: Script kiddie mistake; only finding reported in news

Q3 2021 – multi-site/service credential harvesting

Q1 2021 – Others – use info to compromise

Q3 2020 – TA sells access to others,
commercial malware, rampant key loggers,
memory scrapers

Q1 2020 – TA lock in remaining exfil,
constant streaming, warnings/notifications
from LE / customers

Q3 2019- TA has multiple backdoors (RATs)
multiple Tas, multiple web shells

Q1 2018 – First discovered TA activity

What happens after a breach

ENTERPRISE KNOWLEDGE PARTNERS, LLC

EKP. Because what you don't know CAN hurt you.

- All the stages of grief ; epiphanies, face palms, blaming, self-victimization
  - Some people get fired – not always the right people
- Immediate fixes to previously known problems and delayed projects
  - Budget and resources are no longer an issue
  - Deprecating and replacing legacy systems takes 30 days after 5 years of arguing
- The board is paying attention to cyber
- Lots of audits
- Company produces better product, a better service, trains employees, more efficient operations - all the basics in place
  - A far more costly and unnecessarily painful journey
- **Return to pre-breach culture in approximately two years.**

What happened leading up to the breach

ENTERPRISE KNOWLEDGE PARTNERS, LLC

EKP. Because what you don't know CAN hurt you.

- Budget/investment did not prioritize security, compliance as part of the devops and normal course of business
- No consistent enforcement of the basic security hygiene
  - "We have a policy. Checked that box!"
  - "We passed the pen test for HIPAA/PCI!! – We limited scope to the IPs to the bare minimum, the ones we knew would pass"
  - "We use the cloud – the cloud provider has a SOC2 on its web, so we are good."
  - "Those security guys are really annoying/paranoid – they keep me from doing my job." CTO/CFO/CIO overrides security.
  - "If you don't open those ports [on corp network], I'll send my entire team [SW engineers/DBAs] to Starbucks to work"
- Over-reliance on tools and third parties
- SIEMs was installed – minimal configurations/ingestions
- Lack of systematic enforcement – some departments were off limits to security
- My personal favorite (SW Engineering) – "Yes! Everyone on my team needs full access to production in order to support the customer!"
- Security training and policies were present, but considered a necessary evil
- **AUDITS were consistently under-scoped or findings were temporarily fixed**

Every compliance violation or security incident started with lack of **basic** security hygiene.

Every breach began with a **basic** cultural mistake: missed or ignored alert, unenforced policy violations.

The most successful, long running breaches are caused by **basic** human lack of judgement, errors, lack of qualified resources and a basic lack of curiosity

Asset Management

ENTERPRISE KNOWLEDGE PARTNERS, LLC

EKP. Because what you don't know CAN hurt you.

- Before the breach was discovered:
  - Asset management scanning and log monitoring was limited to assets determined in scope for PCI/HIPAA.
  - Assets in scope did not include security appliances, infrastructure/operational services, developer tools
  - Minimal security policies and controls applied to Non-production environments.
  - No sBOMS: Lack of inventory for APIs, minimal configuration documentation or validations.
  - Software engineers who expose internal service names, IPs, hard coded credentials in code sharing/OS platforms(pastebin, github, slack, stack overflow, etc.
  - Unusual behavior noted in non-production environments
- Cyber investigation findings:
  - Surprising results from comprehensive scans, forensic images
    - Legacy / old / test services, VNETS, VMs, appliances, RMM agents not monitored, never removed
    - Unauthorized assets, apps and services running, web shells on externally facing web servers
  - Lots of warnings, errors, and failed services on assets that were dismissed or not collected.
  - Unpatched vulnerabilities cloud, web app servers, jump servers
  - Malicious APIs, embedded URL redirects hard coded, rogue DLLs, services

Basic Cyber Hygiene: You can't protect what you don't know you have.

End-Point Management (Access Management)

ENTERPRISE KNOWLEDGE PARTNERS, LLC
EKP. Because what you don't know CAN hurt you.

- Before the breach was discovered:
  - Cultural tendency to approve elevated privileges and local admin rights by default; liberal BYOD policy
  - Emphasis on doing whatever is needed to ensure sales, executives, developer work has no impediments
    - Allow personal use, social media and minimal controls on personal, non-work related browsing
    - Executives balked at scanning of USB devices, MFA
  - Turning off end point alerts because SOC/Help Desk/IT was overwhelmed
  - *Multiple complaints* of end point issues, successful phishes, credentials compromised throughout the organization
- Cyber Investigation findings:
  - Persistent LSASS running on multiple devices (re: key loggers, memory scrapers)
  - Alerts found the compromises - dismissed as false positives; ignored clear evidence of insider threats
  - TAs had multiple compromised vectors for many months/years on endpoints (open RDP ports, harvested SSH certs, hard coded credentials)
  - Compromised and bypassed VPN connections, lack of encryption, total compromise of AAD
  - Mobile - compromised downloads, connected to corporate network, no MDM

Basic Cyber Hygiene: No consistent systemic control of endpoints

Access Management

ENTERPRISE KNOWLEDGE PARTNERS, LLC

EKP. Because what you don't know CAN hurt you.

- Before breach was discovered:
  - Shared accounts, email forwarding allowed; no admin account review or changing of credentials
  - Hard coded credentials and keys in services
  - Pressure to skip or cut short validation of supply chain and allow developers to work, products or services to
  - Temporary fixes to audit findings; minimal desire (arguing) about wanting to know if compromise had already occurred
  - MFA not enabled (internally), backdoors to systems built by software engineers
  - Lots of successful, "one off" phishing complaints dismissed as "flukes"
- Cyber Investigation findings:
  - Rampant number of web shells; harvested administrative accounts; key loggers; memory scrapers
  - Enterprise developed authentication bypass mechanisms used "routinely" by TAs
  - Fileless malware rampant throughout organization
  - File configurations changes, installed chrome browsers, scripts running using admin user creds

Basic Cyber Hygiene: No consistent, systemic enterprise access control

Network Security Segmentation

ENTERPRISE KNOWLEDGE PARTNERS, LLC
EKP. Because what you don't know CAN hurt you.

- Before breach was discovered:
  - Blind/implied trust; *over reliance* on perimeter controls
  - Production open to non-production, devops moves with no scanning, cultural emphasis on speed to production; info sec teams had minimal access to devops tools, sources
  - Minimal or no network monitoring in non-production; multiple SIEMs without correlation or no logging/monitoring
  - Convenience or practical, enterprise security; overuse and easy access for IT to bastion hosts, jump boxes
  - Corporate culture network fiefdoms - no centralized visual control over entire network, no deployed network arch standards
- Cyber Investigation Findings:
  - TAs had uninhibited ability to traverse the network
  - Weaponization of infrastructure and security appliances; agents and appliances used to traverse the network and establish
  - Credential harvesting services/tools deployed throughout network
  - Compromised non-prod systems/networks; multiple networks used as a botnet
  - Network traversal via open RDP or equivalent between instances/vnets
  - Backdoor Service bus used by IT exploited by TA

Basic Cyber Hygiene: Implement external and internal network segmentation

Logging and Monitoring

ENTERPRISE KNOWLEDGE PARTNERS, LLC

EKP. Because what you don't know CAN hurt you.

- Before breach was discovered:
  - Selective, perceived high-risk resources and only specific events logged and monitored.
  - Ingress traffic and activity focused
  - Lack of enterprise correlation; fiefdoms
  - External warnings dismissed because of lack of available evidence to validate
  - Logs ONLY used for security – not enterprise wide; co-dependent relationship on third party vendors
- Cyber investigation findings:
  - Ability to detect a compromise determined to be "woefully inadequate"; TAs able to change configurations
  - Time and resource intensive to re-correlate logs, find IoCs, contain the threat, can't find patient zero
  - Total RAT infestation, web shells, started on non-CDE, non-PHI/non-CDE systems; undetected due to lack of monitoring; misconfigured security appliances
  - Web shells on externally exposed servers with TA traversal to internal network – completely missed *for years*
  - TAs ran vulnerability scans using enterprise tools and services – as admins, capitalized on internal vulnerabilities

Basic Cyber Hygiene: Logging and Monitoring to detect baseline anomalies

IR Plan

ENTERPRISE KNOWLEDGE PARTNERS, LLC

EKP. Because what you don't know CAN hurt you.

- Before breach was discovered:
  - Tabletop test only (no functional, purple testing), too many leaders and no doers in the test
  - Policies and procedures checked all the boxes; no one knew the policies; not used as a baseline for validation or testing
  - Dismissal of test scenarios due to over confidence in system
  - Corporate culture based upon fear: "kill the messenger", blame
- After breach findings:
  - Confused, political response that delayed action
  - No established procedure to remediate; IR plan and procedure abandoned
  - Political push to prematurely announce a root cause leading to soiled artifacts, no OOB, inadequate use of external counsel
  - Limited investigation scope = wrong conclusions
  - This wasn't the first breach, they had been successfully compromised up to five years earlier, repeat attacks, multiple TA group personalities and skill sets, access information available on multiple darknet channels/forums.

Basic Cyber Hygiene: The IR plan must be a functional, constantly plan that can be used

Conclusion

ENTERPRISE KNOWLEDGE PARTNERS, LLC

EKP Because what you don't know CAN hurt you.

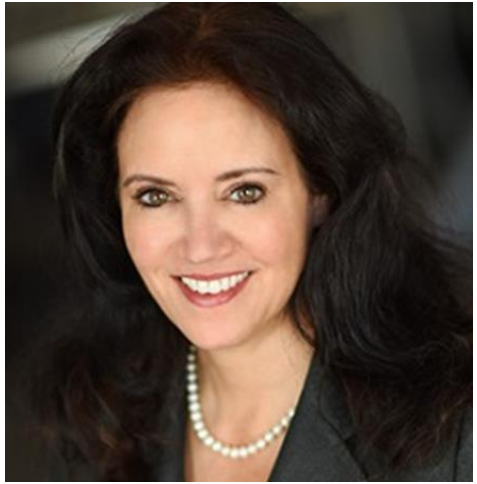
Most threat actors walk through the front door because of lack of basic security hygiene:

- Minimal or no asset management and identification
- Lack of access management
- Lack of network segmentation
- Inadequate logging and monitoring
- Inadequate IR Planning

Those that have successfully made basic cyber practices the baseline:

- More efficient operations, reduced costs
- Adapting to change is easier, faster, less costly
- Employee recruiting is easier, retention is higher
- ***They still have compromises*** **– with less impact, faster detection, less damage**

Mary Frantz
Enterprise Knowledge Partners, LLC
(952) 496-2460
maryf@ekpartner.com



ENTERPRISE KNOWLEDGE PARTNERS, LLC

Because what you don't know, *can* hurt you