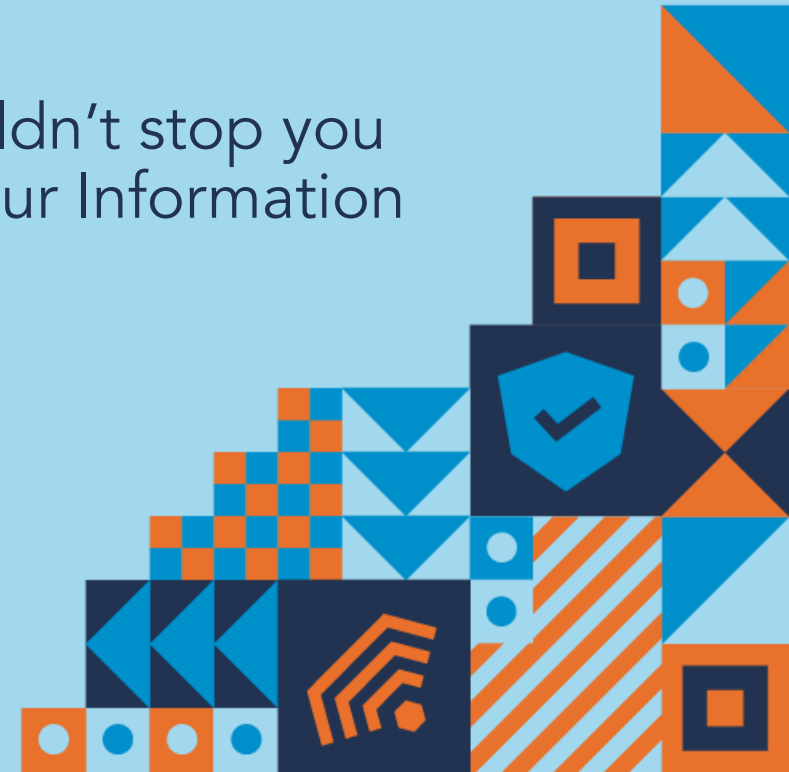
MATURING YOUR PROGRAM WITH A SMALL TEAM

Numbers help but the lack of a large team shouldn't stop you from making meaningful progress in maturing your Information Security Program



Quick background

- When I started at a small online retailer/consumer lending organization, we had:
  - 11 infosec staff
  - 3 locations
  - 1700 employees
  - No cloud presence
  - $1.2 billion in annual revenue
  - Just starting to have dev teams move to agile
  - Immature security program
- 2 years later, after an acquisition and layoffs, we had:
  - 6 infosec staff (at one time as low as 4)
  - 11 locations
  - 3000 employees
  - AWS and Azure/O365 presence
  - $2 billion in annual revenue
  - Agile across all of technology and full DevOps practices

Security Program details (pre-acquisition)

- SecOps: old SIEM, no automation
- Incident Response – informal and undocumented
- InfoRisk
  - Big, annual risk assessment
  - Risks known by InfoSec and no one else, and only somewhat documented
- Project Risk
  - Attend/participate in all we can
  - Document risks and requirements with no follow-up
    - Hope the project met all the requirements
- AppSec
  - SAST scans, 24+ hrs to get results, no CI/CD integration
- Vulnerability Management
  - Scans being run but teams not using the output to ensure patching is working
- IAM
  - Enterprise tool implemented but only 5 annual user access review capabilities enabled
  - Privileged Access Reviews performed manually – 1FTE per year to perform
- Policies were OK and awareness trainings were probably the most mature portions of the program
- Data Governance – didn't exist

Where to start

- 2FA
- Policies
- Document risks
- Incident Response

Policies

- Pick a framework to align your policies towards
  - NIST
  - CSF
  - ISO
  - CSA
- Make sure your policies talk about what you do (don't set policy language to require where you want to be)
  - Two factor authorization must be implemented on all externally accessible web sites and portals vs. Two factor should be implemented (where feasible) on all…
    - Document exceptions to this and get them added to your enterprise risk register
- It is ok to add language to your policies that talk about where you are going
  - It is <insert company name here> desired state that upon approval, automation drive the change into production with proper alerting to the necessary teams. Controls must be in place to detect and alert on changes not occurring via automation.
    - Enforces SoD but prevents delays in deployments
    - It is more secure when implemented correctly
  - Use this language to start setting expectations for the future without requiring it today.

Two factor everything

- VPN
- Azure/O365
- AWS root accounts
- Administrative access and functions
  - Include DevOps automation
- OWA
- SaaS applications or portals that house confidential or sensitive information
- Where you can't, document in your risk register

Risks

- Start with Excel and build a risk register (3 months)
- Keep adding and changing as you become aware of new or mitigated risks.
- Get rid of the big annual risk assessment
- Use monthly risk meetings[1] with a defined team (network, devops, development, legal, compliance, etc.)
- Use these meetings to make decisions
  - implement mitigating controls
  - accept the risk
  - document an exception (policy related issues only)

[1] Learned this from Yan Kravchenko, formerly CISO with Atomic Data

Incident Response

- Do you have documented Incident Response processes or procedures?
- Do you have a defined CSIRT team?
- Do you run annual IR table top exercises?
- How are you leveraging your Cyber Insurance policy and Insurer?
- Think outside the box

AGILE

- Sprints vs. Kanban
- Automation
- DevSecOps

Agile

- 2 weeks sprints aren't for everyone
- Consider Kanban boards
- Security Champions vs project risk assessments
- Review the security of the CI/CD pipeline with DevOps
  - Identify risks
  - Agree to how and when to resolve
  - Add to risk register
- Implement SAST tools into CI/CD pipeline
- Quarterly meetings with dev team or dev chapter leads
- Partner with development and devops to implement agile tools that bring about large security improvements

Automation

- Find a way - whether internal resources (staff add) or external for singlular projects
- SIEM confirmation
  - “Are you logging all of production?”
  - Do you have automated SIEM response capabilities?
    - Restarting SIEM agents on servers that aren’t responding
    - Quarantine devices VPN’ing in that aren’t patched, no AV/outdated AV, etc.
    - Bulk agent removals from non-production servers
- Automate audit related functions
  - Privileged access reviews
  - 90 day inactivity account disabling
  - User access reviews
- Additional security testing added to CI/CD pipeline (fuzzing, TLS verification, etc.)

Final Pieces

- Awareness
- Data Governance

Awareness

- Beyond annual training, implement a monthly newsletter.
  - Keep it user focused for the regular monthly newsletters
  - Publish business line specific newsletters when threats are identified
    - Phishing campaigns going at HR and Payroll to change W2/W4 or address information
- Phishing campaigns
  - Run quarterly
  - Track progress
  - Those who fail get an email with awareness training
  - Those who fail 2 or more times in a rolling 12 month period must take phishing awareness training in your LMS or equivalent.

Data Governance

- Start small
  - get an inventory of your structured data
    - SQL, Oracle, Postgres, DynamoDB, RDS
    - Task your DataOps/DBAs to identify owners for every database
    - Perform annual access reviews (local accounts and AD/LDAP)
  - Have access reviewed for a single file share. Add a new file share each month or quarter.
  - Fix access as you go along which may slow you down. So what? You're making progress.
- Implement email DLP
- O365/Azure – Azure Information Protection, DLP, etc.

Cloud cautions

- Infrastructure as code: cool, but a lot to consider as it relates to SIEM, vulnerability management, and access control
- O365/Azure – SIEM integration is more than a single API connection
- AWS – log consumption into your SIEM, parsing logs, and alerting is not easy.
  - While you aren't going to get your org to wait until you have the needed maturity in your security program, there are going to be new risks associated with cloud as you can't easily extend your current on-prem capabilities to the cloud. Get them in your risk register.
  - Generally, you need to build new versions of your current capabilities and controls to get the same visibility and security.

Security Program status after I left

- SecOps: new SIEM with some automation capabilities implemented.
- Incident Response – documented with annual training and table top exercises.
- Informaton Risk
  - Monthly risk meetings with a working group composed of representatives from all Infrastructure teams, development, Compliance, and Legal.
  - Information risks documented in what I called the enterprise information risk register.
  - Risks were approved by a committee (Informaiton Security Coucil) made up of CFO, GC, Legal, Infrastructure, CIO, and Compliance.
    - This committee met quarterly or as needed.
  - Held quarterly meetings with the individual leaders of each infrastructure team to talk through their adherence and maturity to our policies for all their technologies.
- Project Risk
  - Attend only major projects (4-6 per year)
  - Implemented Security Champions in each development/business squad
  - Document risks and requirements with no follow-up
    - Hope the project met all the requirements

Security Program status (continued)

- AppSec
  - SAST built into the CI/CD process for all development
  - Results are nearly immediate
  - No Critical or High findings in production (internal and external faced applications)
- Vulnerability Management
  - Scans run against PCI scope weekly
  - Non-PCI run monthly
- IAM
  - 80% of all Privileged Access reviews run through our IAM tool (40% FTE savings)
  - Provisioning capabilities for all AD automated along with 1 key system
- Policies have been aligned with CSA and mature
- Awareness trainings and communications occur regularly
- Data Governance – better with plans to improve greatly

Questions?

SECURE360

Twin Cities

Secure360.org

#SEC360