We Need Security Staff

NALIT PDS 2018

Ronda Tentarelli and Mike Norris, Washington

LEG TECH
SUPPORTING A CONNECTED LEGISLATURE

We had an audit

- Underwent independent security audit Spring 2016.
- Set up a Security Team.
- As we addressed the audit findings, we determined that we could not meet our goals with staff who worked on security along with the rest of their jobs, however well-intentioned.
- Reached out to organizations for information about setting up a security program.

The Legislature figured it out

- Events in the news, especially Equifax breach
- Internal awareness heightened
    - Security awareness classes and materials
    - More sophisticated phishing attacks

Gartner's Advice

- An organization should have one dedicated security person for every 30 IT staff.
- Gartner recommended that we have two – a Security Administrator and a Security Architect.

Security Administrator

- Possess IT project management skills
- Have ability to work policy areas with IT and business leadership
- Maintain focus on security initiative
- Establish governance for IT security
- Understand business requirements
- Assess risk – how secure do we need to be?
- Take lead on incident response

Security Architect

- Have a broad understanding of technology (high level)
- Communicate to IT on how to implement controls
- Ensure efforts aren’t duplicated
- Coordinate security work
- Recommend technical solutions/goals (high level)
- Others execute the work

Security Team's recommendation

- Hire a Security Administrator
  - Need the focus.
  - Lack the staff to work with LEG-TECH and legislative management to develop policy, set priorities, and execute.
  - The person should report directly to the Director to avoid undesirable influences as a result of working in a specific group.
  - Current staff can fulfill the duties of the Security Architect.
  - Current staff can perform the technical implementation of controls and infrastructure.

Interviewing

- What appeals to you about this position? What is the first thing you would want to know before you would accept the position?
- What do you feel is the biggest security threat in a typical organization?
- How would you measure the effectiveness of a cybersecurity program?
- Have you ever implemented a cybersecurity program? Can you provide an example of a cybersecurity policy that you have developed?
- Describe the security frameworks that you have worked with. Why were these frameworks chosen? Are you interested in working with the NIST security framework?

Interviewing

- Tell us about a time you were involved in a security incident. Describe the situation, how you handled it and what you learned from it.
- Have you ever participated in a security audit? Can you tell us about it?
- How would you assemble a security team comprised of staff whose primary focus is not security?
- Describe a time when someone disagreed with a security control. For example, a customer did not want to apply workstation security patches each month. How did you work through it?
- With security monitoring and detection devices comes an exorbitant amount of data. How do you keep up with the analysis of the data with limited staff?
- What are your thoughts on enforcing security controls on end-user devices (devices not owned by the agency)?

- Twenty-two people applied.
- We interviewed four people.
- We passed one person to the second round.
- From posting to offer accepted was six weeks.

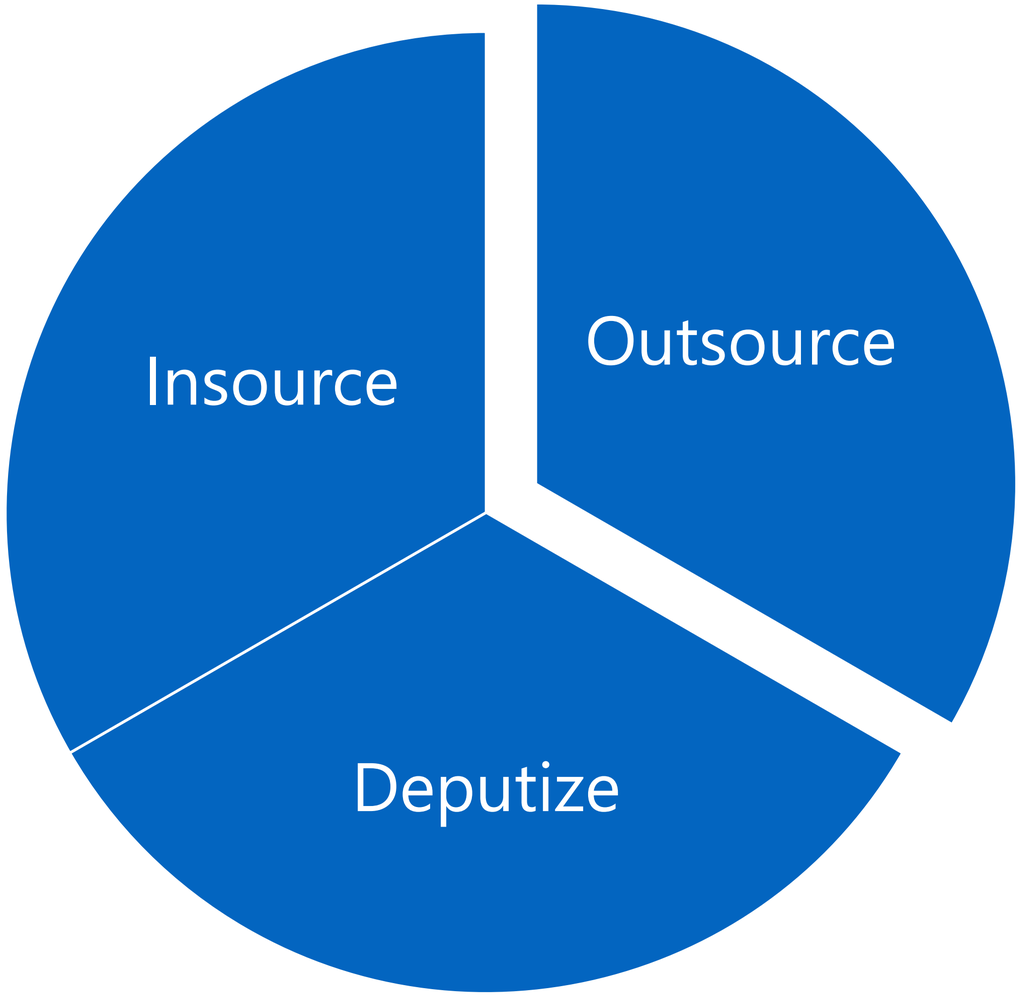
The Result

- He’s sitting here beside me.
- We were really lucky – in addition to Mike’s experience as a security professional, he had worked for the Legislature early in his work life.

Filling Needs

- You can see the team had a role and function in mind. Before you start this endeavor, have a goal or need in mind.
- Consider:
  - Temporary CISOs or security admins offer a unique opportunity to create function and scope for a security program.
  - Utilizing contractors or firms to help define your security need provides time to find the right person with the right skills.
  - Be careful as many firms are there to direct you to purchase more of their services.
- Event-Based:
  - Waiting for an event is too late. A lot of damage can be done between an event and a hire.

Staffing a Security Team



LEG TECH
SUPPORTING A CONNECTED LEGISLATURE

Insourcing

- Hiring New
  - Know what you want.
  - Hiring can be a long process – be patient.
  - Look for major certifications, but fit is more important than degrees.
- Promoting from within
  - This approach has both positives and negatives.
    - A known work ethic and institutional knowledge.
    - A lack of experience and reputation.

Outsourcing

- Be very deliberate and thoughtful.
- Can be a great back-fill for specific functions.
- Can be a good way to gain industry knowledge and experience.
- Can be a good way to test out an employee before you hire them.

Deputizing

- I don’t recommend deputizing to manage the security function, but there are always areas where you need to rely on other folks to address security issues and risks.
- Can be a good way to spread security concepts and training.
- Employees will start asking questions and you can change behavior.

Expectations

- A security person will not keep you from having security issues. You want to have the best person to address those issues when they come up.
  - Old security saying: “You cannot stop a targeted attack, you can just respond to it.”
- Rome was not built in a day.
  - It will take time to implement a program.

Staff to Strengths and Weaknesses

- No one is an expert in all security fields, and if they say they are, they are lying or their knowledge is not very deep.
- If you have someone who is an expert in infrastructure, look to hire someone who is a privacy or policy expert.
- Avoid stretching someone too thin.

Final Thoughts

- You don’t need to stick to one approach – you can mix and match based on need.
- Be deliberate – know what you are looking for and what problem you are trying to solve.
- Set appropriate expectations – surprises will happen.
- Staff to strengths and weaknesses.