JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

Incident Response Teams

CYBER INCIDENT RESPONSE

Creating the Team

- Members are permanent or temporary
- Core team is cybersecurity professionals with incident response experience
- Temporary members brought in for specific cases (like a DB Admin for SQL)
- Smaller organizations have CSIRT as a collateral role in addition to their day job

What does management do?

- Active role in an incident response
- Ensure team has funding, resources, and expertise needed to conduct incident response
- Make critical business decisions
- Communicate with legal or news media
- Communicate with key stakeholders

So, who is on the CSIRT?

- Leader is a skilled Incident Responder
- Subject matter experts
- IT support staff
- Legal counsel
- Human resource staff
- Public relations and marketing staff

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Can you outsource the CSIRT?

- Retaining a third-party gives you instant capability without daily resourcing
- Can be very expensive
- Ensure your organization is comfortable with the third-party's guaranteed response time
- Agree upon the scope of work to be performed

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Scope of Control for a CSIRT

- What would trigger activation of CSIRT?
- Who authorizes the activation?
- Do they respond for all parts of the organization, or just specific ones?
- Can CSIRT talk to law enforcement?
- Can CSIRT talk to the media?
- How would CSIRT escalate an issue?

Testing the Teams

- Plans without testing are ineffective
- You must ensure the teams are trained and ready for an incident response
- Testing allows a walkthrough of the policy, procedures, and playbooks
- Can be combined with a penetration test to simulate a real attacker