Disaster Doesn’t Have to Be Debilitating

by Brad Nigh | CISM, CISSP, CCSFP, CSSA, ITIL, MCSA
Director of Professional Services & Innovation
Agenda

- Intro
- Ways to communicate more effectively
- Where do I start?
  - Set expectations
  - Aim for defensibility
  - Differences in DR plans
  - How to measure effectiveness and improvement
- Everyone’s favorite: POLICY!
  - What should you include in your DR policy?
- Conclusion
- Questions?
Introduction
About Brad, FRSecure, and this presentation
Intro: Brad Nigh, Director of Professional Services & Innovation

• 20+ years of overall IT experience, started with FRSecure in 2016
• CISSP Mentor Program Lead
• FRSecure Workshop Series Lead
• Co-host of UNSECURITY Podcast with Evan Francen
• ISC2 Safe and Secure Online volunteer
• Wayzata Schools COMPASS program Cyber Security Mentor
• Passionate about information security and happy to be here!
Intro: FRSecure

• Information Security Consulting and Management company. It’s all we do.

• Our core services include:
  • Security Risk Analysis – using FISASCORE®
  • Social Engineering Services
  • Penetration Testing Services
  • PCI QSA Services
  • Incident Management Services
  • HITRUST Services
  • Information Security Training & Awareness
  • vServices (vCISO, vISO, and vISA)

• Methodology fanatics, mentoring champions, and product agnostic.
Intro: Things to Know

• This presentation contains generalizing and stereotyping – it’s necessary
• Your executive team wants to better understand security
• Patience is key
• You are intimidating
• You have a greater responsibility
Ways to Communicate More Effectively

You need to not just be heard, but be understood
Ways to Better Communicate

1) Dumb it down – there, I said it.
   • Instead of “RTO” use “How long can this be down”
   • Instead of “RPO,” use “How much work can we afford to lose”
   • Instead of “ram the gigabytes (or whatever),”* speak to the objective of
     the tech/control
   • Example – VTL= Low cost way to get rid of tapes and make backup
     and recovery faster

*Thanks to our President, John Harmon, for this beauty.
Ways to Better Communicate

2) Align with business
   • Get in the room!
     • Do you know where your business is going and why?
     • How can you build a DR strategy around an uncertain future?
     • Get up to speed – don’t wait for them to come to you!
Where Do I Start?

At the beginning, naturally
Setting Expectations

A story: Evan (our CEO) used to work for a big pharma company. Every now and then, the CEO would ask “are we secure?” Evan would say “yes, sir” because explaining things was too hard.

Security is relative, not binary.

The CEO wasn’t “wrong,” but the why was ill-defined. Evan thought his job was to do his best to manage the security risk of the company. The CEO thought Evan’s job was to make the company 100% secure.

They were not on the same page…
Your Goal is a Defensible Position. Perfection isn’t possible.

Eliminate the following phrases from your infosec vocabulary:

- We thought
- We assumed
- We weren’t informed

What would a reasonable person/company do?

- No need to be “unbreachable”
- Living in fear is no way to live
- Business needs > security (healthcare is a great example to follow)

Measure everything

- Be able to demonstrate deliberate, substantive improvement over time

Secure360.org  #SEC360
Differences in DR Programs

• “Traditional:” IT makes decisions
  • Full backup on the weekend
  • Incremental or Differential on weekdays

• Optimized
  • Business (data owner) tells IT (custodian) the requirements for protecting data.
  • IT implements controls to satisfy the business requirement
How to Measure Improvement

• Everyone else has to…

How do you demonstrate security tech ROI?
  • Average incident costs the company 30 man hours to properly recover from = $3,000
    • Last year, we had 10 incidents = $30,000
      • Implemented $15,000 VTL solution to eliminate tapes
      • Average incident now costs 5 man hours, 10 incidents = $5,000
    • Net savings = $10,000

You may be viewed as a “cost center,” but demonstrating that you think this way will build trust because this is how executives and boards think.
Everyone’s Favorite Policy!
Why Policy?

- Policy
  - Sets accountability
  - Formally approved by Executive leadership
- Plan
  - Start somewhere
  - Update regularly
  - Perform scheduled tests
What is Policy, Really?

- An adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence;
- Personnel with the necessary responsibility, authority, and competence to manage an incident and maintain information security are nominated;
- Documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.
What Should Be in Your DR Plan

• Disaster Recovery Plan
  • Purpose
  • Scope and Objectives
  • Emergency Notification Contacts
  • Assumptions
  • Team Member Responsibilities
  • Revisions and Updating Schedule
  • Plan Documentation Distribution and Storage

• Invoking the Plan
  • Plan Triggering Events
  • Assembly Points
  • Activation of the Disaster Recovery Team
  • Employee Communications
  • Instructions for Using the Plan
    • Emergency Alert, Escalation, and DRP Activation
What Should Be in Your DR Plan

• Notification
  • Emergency Management Procedures
  • Alternate Locations
• Back Up Location
  • Emergency Command Center
  • Backups and Offsite Storage
  • Equipment
• External Communications
  • Media
  • Interaction with Law Enforcement
  • Regulatory Authorities
  • Customers
  • Insurance
What Should Be in Your DR Plan

- Financial and Legal Issues
  - Financial Assessment
  - Financial Requirements
  - Legal Actions
- Plan Testing
  - Overall Supervision
- Version History
- Appendix A
  - Disaster Risk Assessment
- Appendix B
  - Business Impact Analysis Summary
What Should Be in Your DR Plan

• Appendix C
  • Additional Documents:
    • Disaster Recovery Plan Overview for Management
    • First 24 Hours Checklist
    • Detailed Restore Procedures
    • List of Staff/Phone Tree
    • Organizational Chart
    • List of Key Vendors
    • Insurance Policy Details & Contact Information
    • Disaster Testing Checklist
    • Information Resource Assets
    • Building Evacuation Information (map of building, evacuation procedures)
Conclusion

Some parting thoughts...
What’s Next?

• TEST!
  • At least annually run a test of your DR plan.
    • Tabletop
    • Technical
  • Learn from these tests and update your plan
  • INCLUDE THE BUSINESS IN THE TEST
Conclusion

• Build relationships – don’t be the “no” guy/gal
  • It’s not your job to make risk decisions
  • Be the person who figures out how to make things happen
  • Don’t use FUD – it makes you less accessible

• 30 seconds is all you get to grab an executive’s attention
  • Do you have a security “elevator pitch?”
  • If not, do you need better words or a less complex program?
The Most Important Thing to Remember

You will never have a “perfect” plan, and that’s ok.
Questions?
Download this presentation:

https://info.frsecure.com/sec360brad
Resources & Contact

• FRSecure.com
  • LOTS of content
  • E-commerce security services (ie: no salespeople)

• UNSECURITY
  • Book – evanfrancen.com
  • Podcast – evanfrancen.com/media/

• Email: bnigh@frsecure.com
• twitter: @BradNigh