



O-ISC '07
Ohio Information Security Conference

Beyond Tabletop: Hands-On IR Testing

Keith Fricke - Cleveland Clinic

Matt Curtin – Interhack



Cleveland Clinic

INTERHACK

■ Keith Fricke - CISSP

- 21+ years IT experience
- Past 8 years InfoSec focused
- Data Security Administrator for Cleveland Clinic East
- Adjunct Professor, MIS Dept., Ursuline College

■ Matt Curtin - CISSP

- Founder & CEO of Interhack
- Specialties in Computer Forensics and Information Assurance
- Expert Legal Testimonies
- Author
- OSU Adjunct Faculty, Computer Science & Engineering Dept.

- Why a Hands-On Test?
- Pre-Test Logistics & Planning
- Defining Our Incident
- The Kick-Off
- The Hand-Off
- Wrap Up & Questions

Why a Hands-On Test?

- It's Like DR Testing
- The best laid plans.....
- Skill Assessment



- Define Objectives
- Type of Incident
- Critical Questions
 - How much prep time & test time?
 - What roles needed for prep & test?
 - Skills needed vs. skills possessed?
 - Equipment needed?



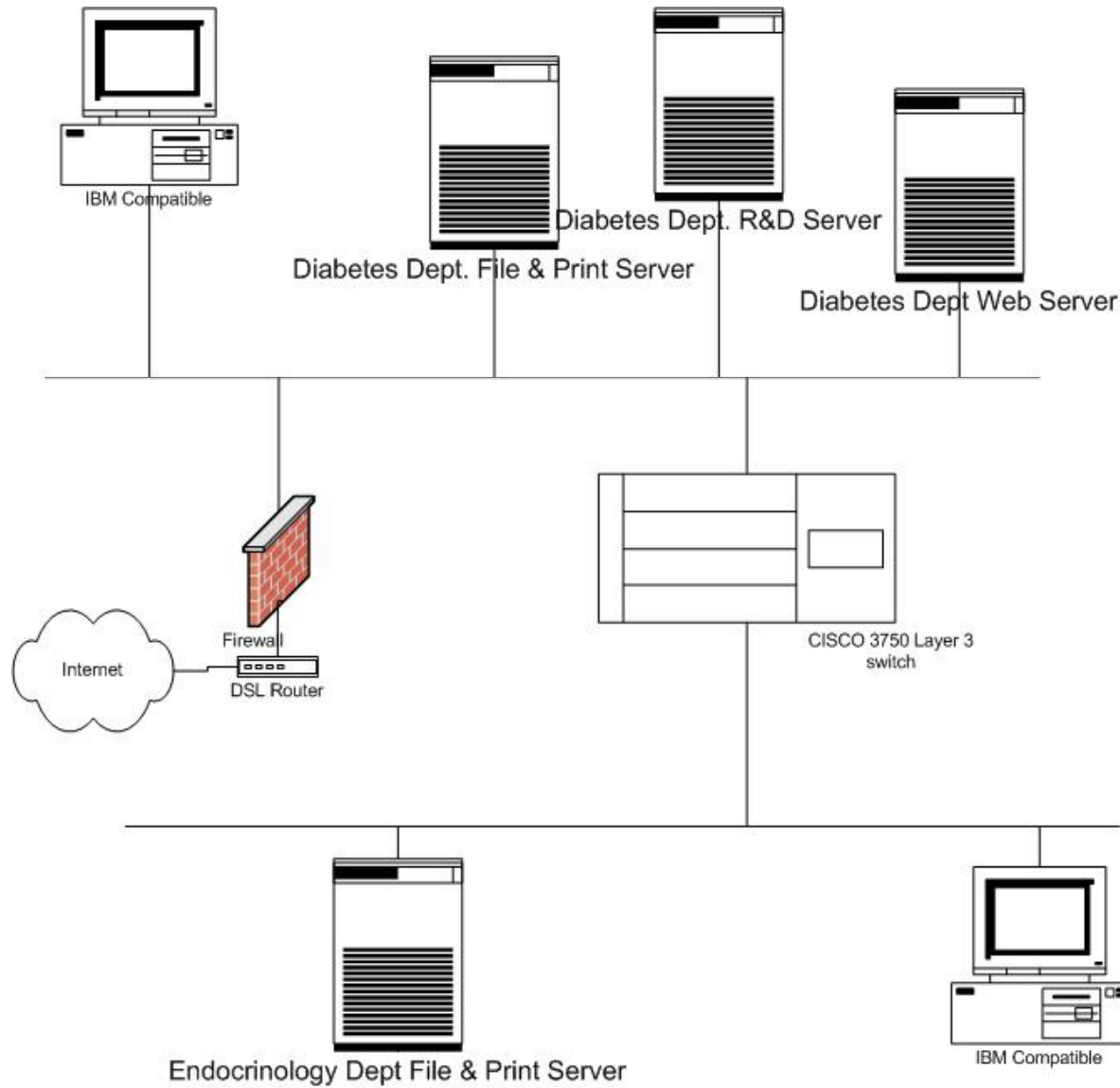


- Test Location & Travel
- Feeding the Natives
- Identifying Assumptions/Limitations

Defining Our Incident

- “Adaptable” Scenario
- Network Diagram
- Answering our Critical Questions
- Objectives and Assumptions

Network Diagram



Answering Critical Questions



- Test time: 8 hours
- Prep Time: Months
- Roles for test:
 - Coordinators
 - Administrative
 - Director, CC Information Security Dept.
 - Manager, Information Security – Central
 - CC Incident Response Coordinator
 - Internal Audit (observe)
 - Technical
 - 1 Network Engineer
 - 3 Wintel/Unix Admin (1 Security champion)

■ Roles for prep:

- Network Engineer
- Security Consultant
- Fricke managed logistics and technical setup

■ Skills

- Network Capture & Analysis
- Windows & Unix administration
- Forensic Analysis
- Management response & leadership

Objectives

- Test our Playbooks
- Skill Assessment
- Recognition of Policy Violations
- Feedback:
 - Value of test
 - Improvements in planning
 - Improvements in execution

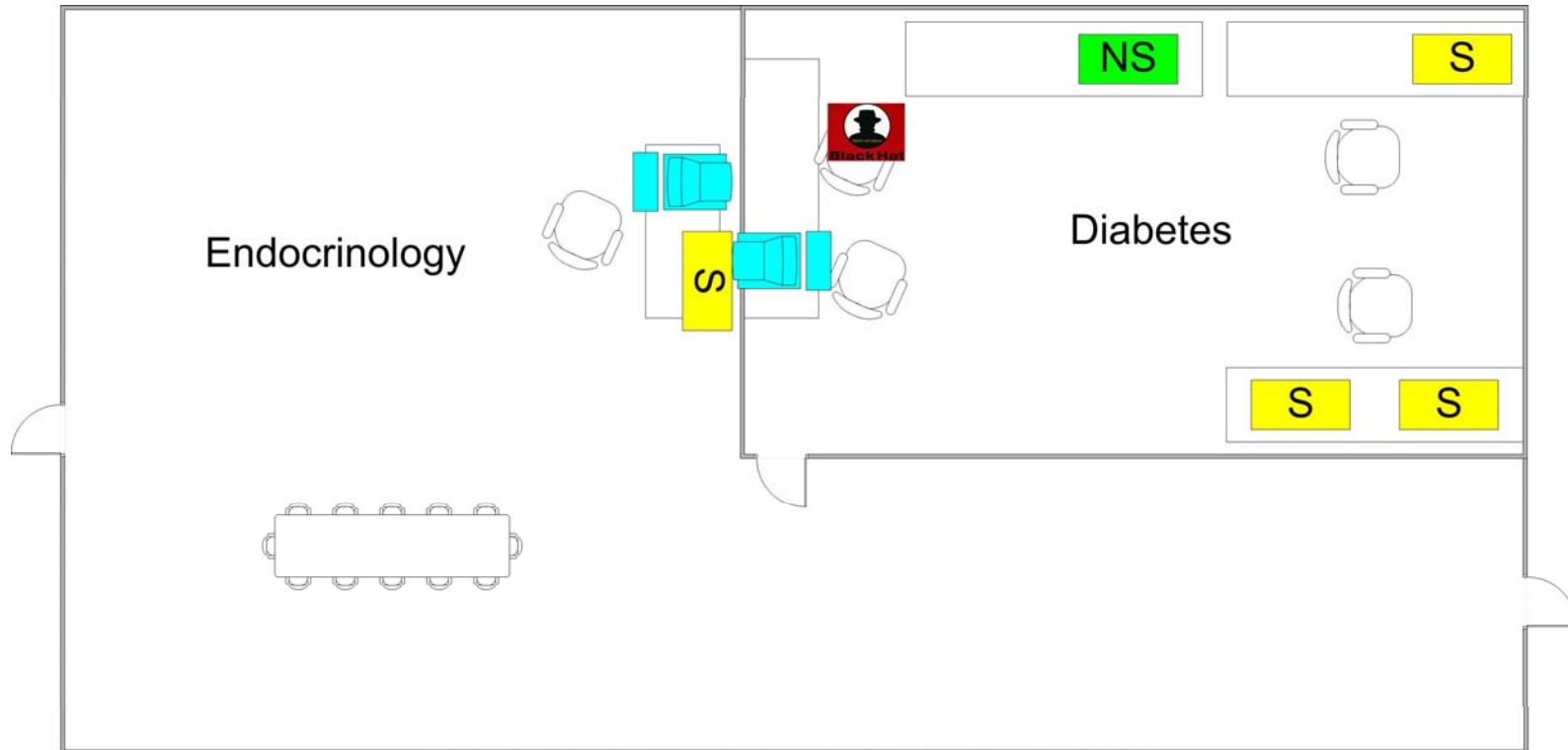


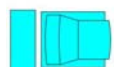
- Diabetes (DB) & Endocrinology (Endo) Dept Staff attending a conference in Canada
- Jan Smith, DB Dept. Admin Assistant out on LOA
- Doris Meeks, Endo Admin Assistant covering both depts.
- Endo & DB – “physically separate”
- Both depts. have own IT staff but CC manages network switch




- Network Switch “located” in closet
- Endo & DB staff all have laptops with them
- No email system or DNS in this test
- File cabinets assumed present
- DSL modem in DB not connected to real circuit – assume it is

Layout of Test Space



 = PC

 = Server

 = Network Switch

 = Matt

The Kick-Off

- Keeping track of who is who
- Start your engines
- 8:50am – Something's fishy
- What would you do?
- Meet Doris
- 9:30am – Sys Admin & Doris chat


Incident Unfolds

- 9:54am – A call from the boss
- 10:10am – Sidebar starts
- 10:30am – New discovery!
- 11:00am – Bob enters
- 11:10am – Surprise!
- 11:15am – Bob calls his boss
Charlie

Incident Continues

- What would you do?
- 11:25am – Lights out
- 11:30am – It's about time!
- 11:45am – Management kicks in
- 12:10pm – Gathering more info

Incident Continues

- 12:55pm – Calling Pete
- Pete and Bob – Your thoughts?
- Winding down
- 1:30pm – Lunch
- 2:45pm - 

Hand-Off to Matt

- Opening remarks at test
- Skill set required for Matt's role
- Leading the Post Mortem
- 3rd Party Perspectives & Assessment

Summary

- Reviewing test goals
- Things we learned
- What Management said
- What's Next?



Questions?

Contact Information



Keith Fricke
Cleveland Clinic
216-738-5121
kfricke@cchseast.org

Matt Curtin
Interhack
614-545-4225
cmcurtin@interhack.com