THE BLIND SPOT
WHAT SHOULD AN EXECUTIVE EXPECT FROM INFORMATION SECURITY?

INTRO
Who am I? Who is FRSecure?

DEFINING THE BLIND SPOT
What does it mean?

3 QUESTIONS & HOMEWORK
What to ask and what answers to accept

STORY TIME
Real world examples of executives getting scammed

Q&A

Speaker: Jim Nash, Information Security Evangelist at FRSecure
- Spreads infosec awareness to audiences across the country on behalf of FRSecure
- Business and elected government background
- Married with 6 kids
- Current citizen legislator (MN State Representative)
- Member of Board of Advisors Metro State MNCyber program
- Member of MN Governor’s Blue Ribbon Panel on IT Reform
- Very happy to be here!
Information security consulting and management company – it's all we do
Based in MN – ~75 employees
Our core services include:
• Security Risk Analysis – using FISASCORE®
• Social Engineering Services
• Penetration Testing Services
• PCI QSA Services
• Incident Management Services
• Information Security Training & Awareness
• vCISO Services
• Methodology fanatics, mentoring champions

DEFINING THE BLIND SPOT

What does it mean?
DEFINING THE BLIND SPOT

Reputational Risk

“It takes 20 years to build a reputation and 5 minutes to ruin it.”

- Warren Buffett

Security is NOT just an IT function

• People are the biggest risk
• People can’t be “fixed” with technology

Security is NOT one person’s responsibility

• Everyone must be involved
• Leaders set the tone; much like every other business function

Security is NOT compliance

• Compliance is doing what you have to do
• Managing risk is what you should do (and it actually works)

3 QUESTIONS & HOMEWORK

What to ask and what answers to accept
THE BLIND SPOT

3 QUESTIONS & HOMEWORK

Question 1: What is our current state?

- **Adequate Answers**
  - We measure our security by (insert method here) and we are somewhere definitively on that scale.
  - We have an assessment in progress that will tell us for sure.
  - I don't know.

- **Inadequate Answers**
  - We passed our audit / we are compliant with (insert regulation here).
  - A long, excruciating, technical jargon-ridden definition that nobody understands.
  - We're good.
  - Our IT provider has us covered.

In short - expect concise answers that speak to your level and position.
This should feel as natural as looking at financial results, sales numbers, etc.

Question 2: What is our future state?

- **Adequate Answers**
  - We agreed as a committee/leadership team that we need to reach a score of X in the (insert method here) way of measuring security risk.
  - By (specific date), we will be done implementing/refining abc initiatives and moving on to xyz initiatives, as we've all agreed.
  - I don't know.

- **Inadequate Answers**
  - We'll be ready for our audit/compliance.
  - We're spending more on xyz technology or support.
  - More jargon you don't understand.

Question 3: How do we get there?

- **Adequate Answers**
  - We have these 2-3 things that are no cost, these 2-3 things that are some cost and these 2-3 things that are costly, but worth it (and why).
  - We agreed as a committee/leadership team to focus in xyz areas and expect X% improvement by a specific date. We will measure success in a certain way.
  - I don't know.

- **Inadequate Answers**
  - By complying with (insert regulation here).
  - By focusing on our technology only.
  - Yet more technical jargon.
Homework

- Go ask these questions, record the answers, and share them.
- Keep an open mind
- Support your team
- Raise expectations
- It’s unlikely you have a security expert in charge of security. Learn together!

---

STORY TIME

Real world examples of executives getting scammed

---

QUESTIONS?

QUESTIONS?

Feel free to get in touch!
- Email: jnash@frsecure.com
- Twitter: @JimNashMN

Thank you!