UP YOUR SECURITY GAME:
3 STEPS FOR EMPLOYEE MONITORING

Evan Francen – CEO & Founder, FRSecure

INTRODUCTION

UP YOUR SECURITY GAME

Topics/Agenda

- Introduction
- Defining Information Security (Correctly)
- People Are the Greatest Risk
- Three Steps to Establishing An Employee Monitoring Program
- Assumed Breach – Be Defensible
- Questions You Have for Me

INTRODUCTION

UP YOUR SECURITY GAME

Speaker: Evan Francen, CEO & Founder of FRSecure and SecurityStudio

- Co-inventor of SecurityStudio®, FISA™, FISASCORE®, and Vendefense™
- 25+ years of “practical” information security experience (started as a Cisco Engineer in the early 90s)
- Have worked with 100s of companies; big (Wells Fargo, US Bank, UHG, etc.) and small
- Have written more than 750 articles about information security
- Developed the FRSecure Mentor Program; six students in 2010/360+ in 2018
- Dozens of television and radio appearances; numerous topics
- Advised legal counsel in very public breaches (Target, Blue Cross/Blue Shield, etc.)

AKA: **The “Truth”**

29th Annual ALAMN Educational Conference
POWER OF 5
Business Partners
Networking
Education
Resources
Community Service

INTRODUCTION

UP YOUR SECURITY GAME

Author of *UNSECURITY*

29th Annual ALAMN Educational Conference
POWER OF 5
Business Partners
Networking
Education
Resources
Community Service

INTRODUCTION

UP YOUR SECURITY GAME

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.

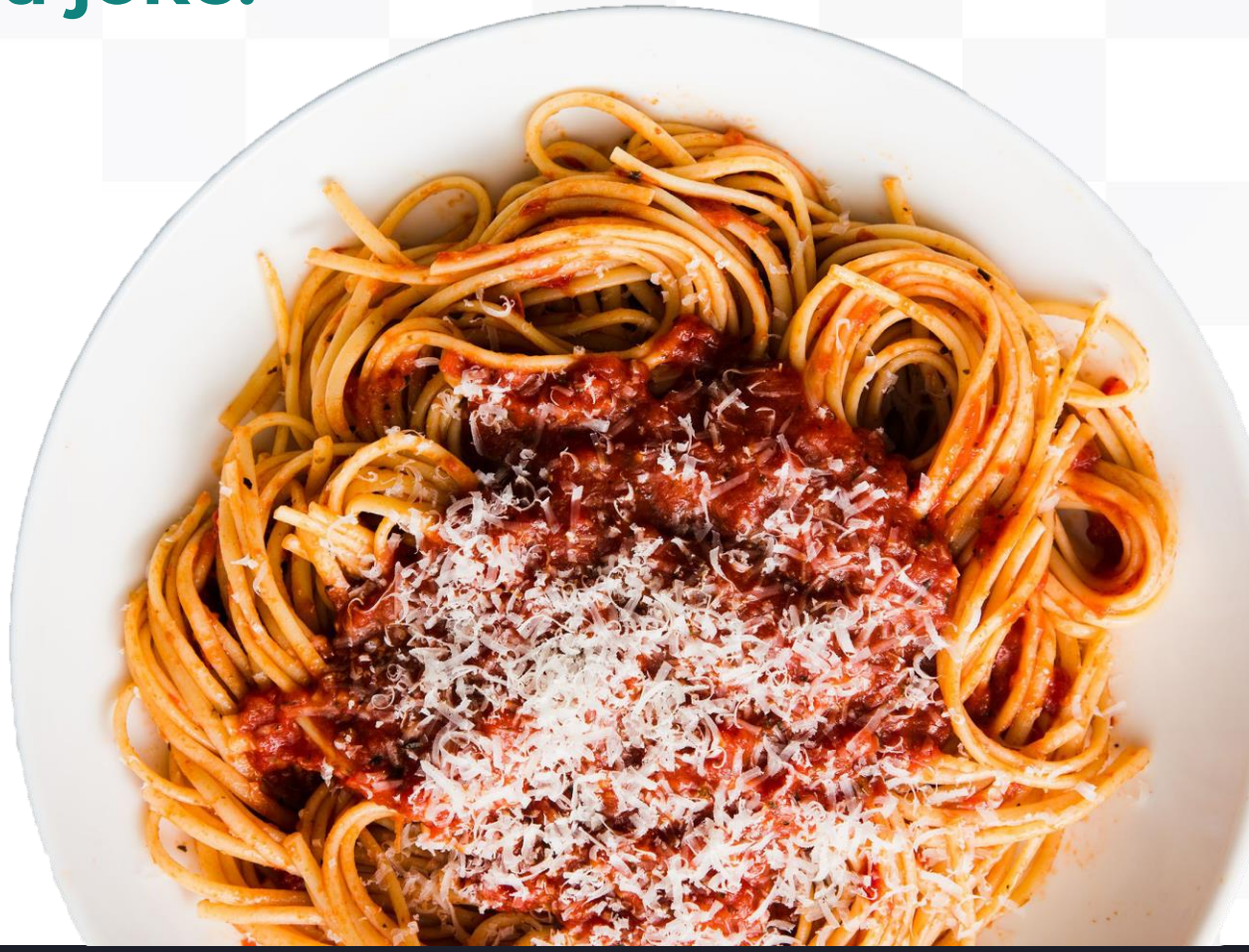
FRSECURE®

INTRODUCTION

UP YOUR SECURITY GAME

Let’s get started, but first a joke.

What do you call fake spaghetti?



29th Annual ALAMN Educational Conference
POWER OF 5
Business Partners · Networking · Education · Resources · Community Service

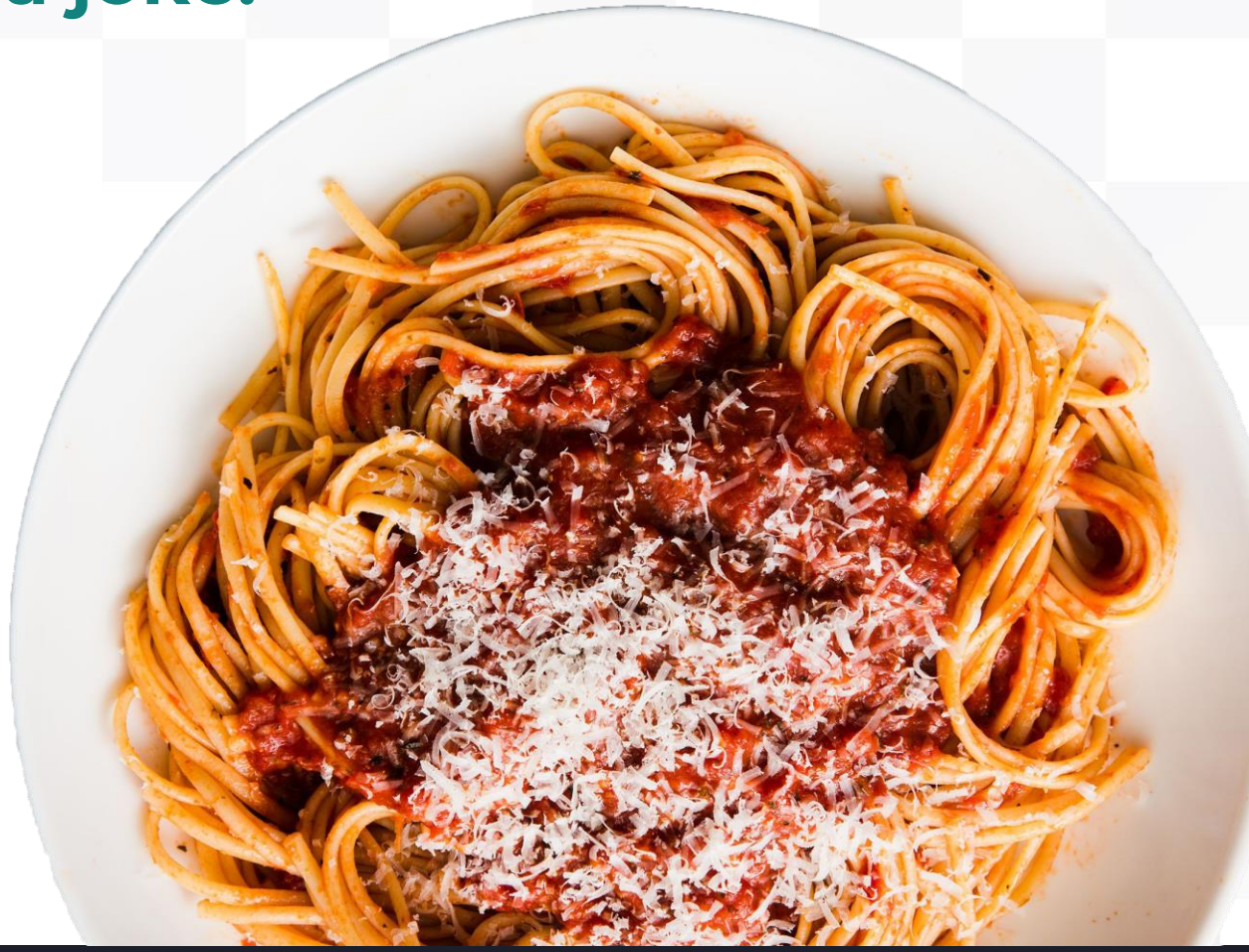
INTRODUCTION

UP YOUR SECURITY GAME

Let’s get started, but first a joke.

What do you call fake spaghetti?

An impasta.



29th Annual ALAMN Educational Conference
POWER OF 5
Business Partners · Networking · Education · Resources · Community Service

UP YOUR SECURITY GAME

Defining Information Security (Correctly)

- Ask 10 “experts” the same question.
  - 10 different answers
  - We’ve got egos, so we all think ours is better. UGH!

- Simplify! – Complexity is the enemy of information security – remember this.

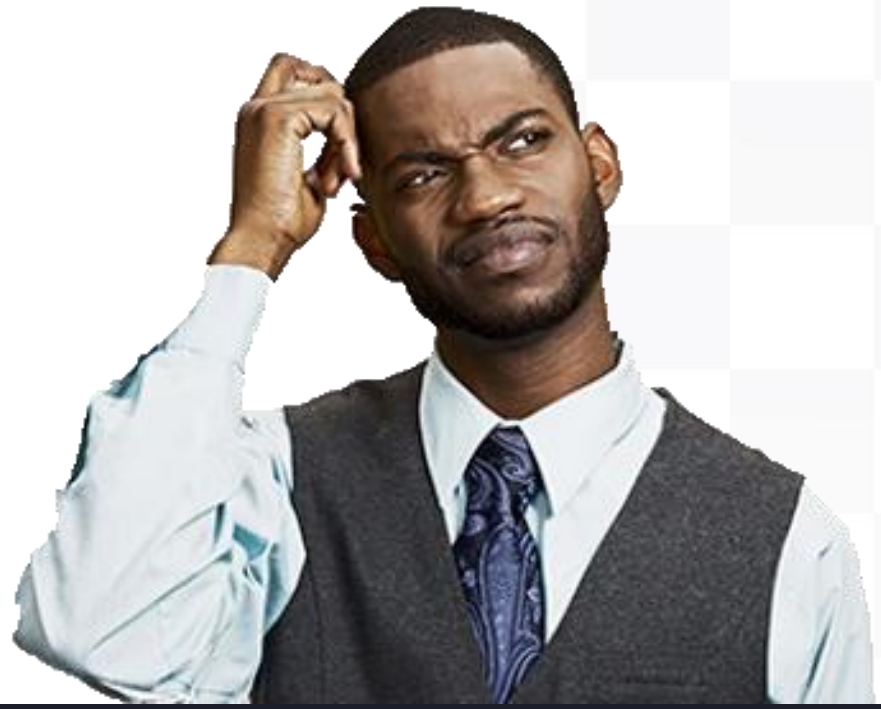
- Our (my tribe’s) definition…

UP YOUR SECURITY GAME

Information security is managing risk to information…

- Confidentiality
- Integrity
- Availability

- Using…
  - Administrative,
  - Physical, and
  - Technical Controls.



UP YOUR SECURITY GAME

Information security is managing risk to information…

- Confidentiality
- Integrity
- Availability
- Using…
  - Administrative,
  - Physical, and
  - Technical Controls.

- **TRUTH:** Information security is about **MANAGING** risk, **NOT ELIMINATING** risk. Much, much different.
- Risk is an overused word, but the meaning is the **likelihood of something bad happening** and **the impact if it did**.
- You manage risk every day. Most of this risk management is automatic and even subconscious.
- **TRUTH:** security incidents and breaches are not completely preventable and should be expected.
  - No matter what you do, you cannot prevent all bad things.
  - What you can't prevent, you should be able to detect and respond to.

UP YOUR SECURITY GAME

Information security is managing risk to information…

- **Confidentiality**
- Integrity
- Availability
- Using…
  - Administrative,
  - Physical, and
  - Technical Controls.

- Confidentiality is about keeping things **secret**.
- Only the people/programs who are authorized to access information are permitted to access information.
- Most people think that this is the purpose of security, but as you can see, it's only one purpose.
- **TRUTH**: Everybody's got secrets. **Everybody**.
  - Personal – Social Security Number, passwords, things that go on in their homes, etc.
  - Business – Intellectual property, customer information, etc.
- This is where privacy lives…

UP YOUR SECURITY GAME

Information security is managing risk to information…

- Confidentiality
- **Integrity**
- Availability
- Using…
  - Administrative,
  - Physical, and
  - Technical Controls.

- Integrity is about making sure the information is **accurate**.
- This is an oft-overlooked part of the definition.
- You make decisions every day based on the information you receive and consume.
- **TRUTH**: Poor information = poor decisions.
- Wouldn't it be nice (sort of) to:
  - Change the balance of your bank account (to the positive)?
  - Change your grades at school?
  - Influence (or manipulate) others with false information?

UP YOUR SECURITY GAME

Information security is managing risk to information…

- Confidentiality
- Integrity
- **Availability**

- Using…
  - Administrative,
  - Physical, and
  - Technical Controls.

- Information must be made available to (authorized) people when they need it.
- **TRUTH**: A business is in business to make money. If we make it harder to make money, we've done something wrong.
- Common attacks against availability include things like ransomware, denial of service, etc.

UP YOUR SECURITY GAME

Information security is managing risk to information…

- Confidentiality
- Integrity
- Availability

- **Using…**
  - Administrative,
  - Physical, and
  - Technical Controls.

- How do we protect confidentiality, integrity, and availability?
- We use different types of **controls**.

DEFINING INFORMATION SECURITY (CORRECTLY)

UP YOUR SECURITY GAME

Information security is managing risk to information…

- Confidentiality
- Integrity
- Availability
- Using…
  - **Administrative**,
  - Physical, and
  - Technical Controls.

- Administrative controls apply to the “people part” of security.
- Policies, procedures, training, awareness, etc. are all administrative controls.
- People are always the greatest risk.
- ***It’s easier to go through your secretary than it is your firewall.***

- **TRUTH**: Information security is **NOT** an IT issue. It’s a **business** issue.
- Policies get a bad rap because people stink at using them.
  - They’re the rules, think a board game.
  - They’re not supposed to be read by everyone.
  - They’re reference documents.
  - They’re supposed to reflect you (your rules).

UP YOUR SECURITY GAME

Information security is managing risk to information…

- Confidentiality
- Integrity
- Availability
- Using…
  - Administrative,
  - **Physical**, and
  - Technical Controls.

- Physical controls are used to protect and detect physical access to the things you want to protect.
- Physical controls are also used to respond to unauthorized access.
- ***It doesn't matter how well your firewall works if someone can steal your server.***

- **TRUTH**: Information security is **NOT** an IT issue. It's a **business** issue.

UP YOUR SECURITY GAME

Information security is managing risk to information…

- Confidentiality
- Integrity
- Availability
- Using…
  - Administrative,
  - Physical, and
  - **Technical** Controls.

- This is the IT part of information security.
- This is also what many people think is “information security,” but they do so at their own peril.
- Technical controls include things like passwords, firewalls, anti-virus software, etc.

- **TRUTH**: Information security is **NOT** an IT issue. It’s a **business** issue.

DEFINING INFORMATION SECURITY (CORRECTLY)

UP YOUR SECURITY GAME

Information security is managing risk to information…

- Confidentiality
- Integrity
- Availability
- Using…
  - Administrative,
  - Physical, and
  - Technical controls.

- So, there you have it.
- What does this mean for you?
- Let's recap the truths quickly:
  - **TRUTH:** Information security is about **MANAGING** risk, **NOT ELIMINATING** risk.
  - **TRUTH**: security incidents and breaches are not completely preventable and should be expected.
  - **TRUTH**: Everybody's got secrets. **Everybody**.
  - **TRUTH**: Poor information = poor decisions.
  - **TRUTH**: A business is in business to make money.
  - **TRUTH**: Information security is **NOT** an IT issue. It's a **business** issue.

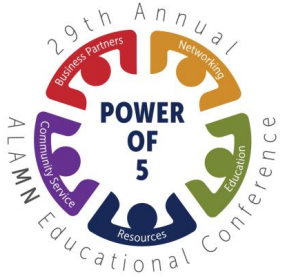
PEOPLE ARE THE GREATEST RISK

UP YOUR SECURITY GAME

Some Supporting Stats...

Inherently we know this; either intentionally or unintentionally.

- **47 percent** of business leaders said human error such as accidental loss of a device or document by an employee had caused a data breach at their organization
  (Source: https://www.cnbc.com/2018/06/21/the-biggest-cybersecurity-risk-to-us-businesses-is-employee-negligence-study-says.html)
- **95 percent** of cybersecurity breaches are due to human error
  (Source: https://www.cybintsolutions.com/cyber-security-facts-stats/)
- Attacks involving cryptojacking increased by **8,500%** in 2017.
  (Source: http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_)
- In 2017, spear-phishing emails were the most widely used infection vector, employed by **71%** of those groups that staged cyber attacks.
  (Source: http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_)
- **41 percent** of people globally cannot properly identify a phishing email.
  (Source: https://www.symantec.com/security-center/threat-report)



UP YOUR SECURITY GAME

Where do you begin?

- Must meet business needs but also **ethical** and **privacy** concern, can be tricky.
- When you establish a monitoring program, you can maintain employee trust by **minimizing** the impact on their privacy.
- You need to avoid the observation of **personal information**, contents of personal email, and details of personal accounts.
- Particularly avoid viewing **protected conversations**, like those between an employee and their doctor or lawyer.
- **Justified** reason for intrusive monitoring - like a security incident or valid request from a manager

UP YOUR SECURITY GAME

Step 1:

Create written policies and employee agreements, and make sure to define what constitutes non-work activity.

For example, an Employee Information Security Policy should include topics like:

- Acceptable Use of Information Resources
- Internet and Social Media Use
- Email Use
- Mobile Device Use
- Privacy (Ontario v. Quon, 560 U.S. 746)

UP YOUR SECURITY GAME

Step 2:

Train your employees on the policies annually, and maintain awareness constantly.

- **Training** is teaching people to do something. **Awareness** is maintaining security as top of mind.
- Cover regulatory **requirements** and your liability or data breach insurance policies.
- After the training has been completed, have your employees **sign agreements**.
- Keep a **record** of who attended training, and when.
- Get **creative**. Corny & quirky = memorable. Make it **fun**. Gamification.

UP YOUR SECURITY GAME

Step 3:

Use technology to automate most of the monitoring.

- Don't let monitoring add a bunch of overhead to your business. **Leverage** technology and focus on the basics first:
  - **Web filtering** services can filter web sites based on categories. Cheap, effective, and they help protect against malware, too!
  - **Data Loss Prevention (DLP)** policies in modern email systems, cloud services, and on endpoints will help prevent data from having an opportunity to leave.
  - High-definition video **surveillance cameras** provide physical monitoring, and are proven to help deter criminal activity in and around facilities. These have a huge bang for the buck!
  - Managers should **review reports** on their employees' web browsing and email activity from firewalls, proxies, and email systems at least quarterly. Reviewing activity can establish patterns - but be careful of privacy violations if you go further and review the contents of employee web and email activity!

UP YOUR SECURITY GAME

Are you defensible?

- If your organization suffered a breach, what things have you done that are **defensible**?
- **Negligence:** A failure to behave with the level of care that someone of ordinary prudence would have exercised under the same circumstances. The behavior usually consists of actions, but it can also consist of omissions when there is some duty to act (e.g., a duty to help victims of one's previous conduct).
  - Is it **defensible** to not do an information security risk assessment?
  - Is it **defensible** to not train your employees?
  - Is it **defensible** to not monitor your employees?

QUESTIONS?

UP YOUR SECURITY GAME

Questions?

Hopefully about security.

Thank you!

For a copy of this presentation,

text **alamn19** to **555888**

Now you know the basics.

...and the basics are what's most important.

Evan Francen – https://evanfrancen.com

- **FRSecure – https://frsecure.com**
- evan@frsecure.com
- @evanfrancen

FRSECURE®