ARIZONA SMALL BUSINESS BOOT CAMP & COLLECTIVE

RESPOND → PLAN → RETURN STRONGER

COSANT
CYBER SECURITY

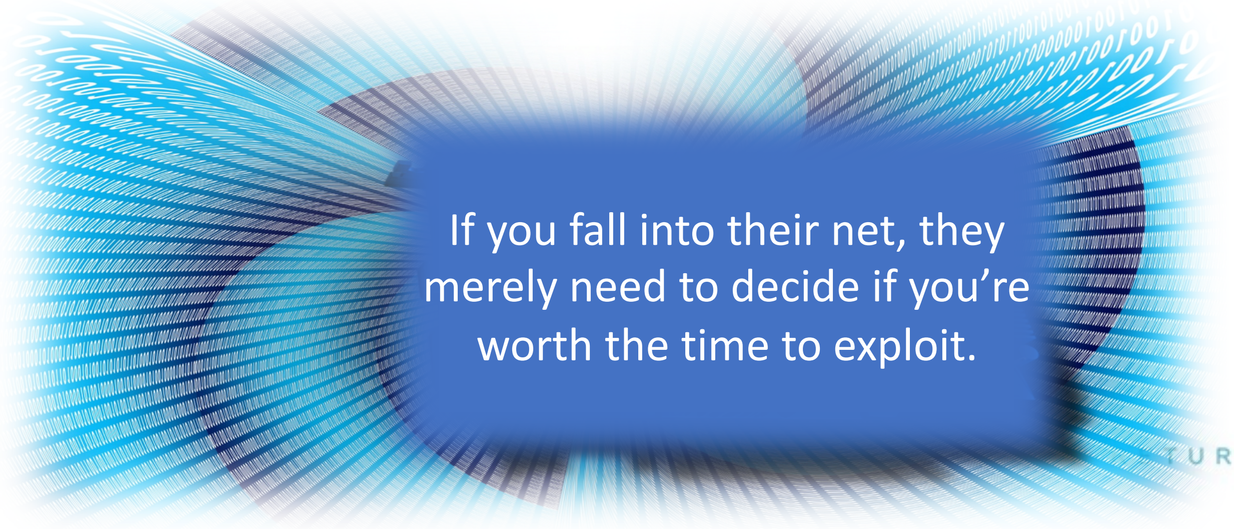
Why Cyber Criminals Don’t Care if you’re a “Good” Target

PRESENTED BY

Mark Kirstein

Myth: I’m too small to be a cybersecurity target

1. Most Cyber Criminals aren’t ‘hunting’… They are “net” fishing
   - Broad campaigns, aimed at catching anyone who is easy prey
   - Automated campaigns
   - Social Engineering based on data-mining intelligence for believability



If you fall into their net, they merely need to decide if you’re worth the time to exploit.

Myth: I’m too small to be a cybersecurity target

2. It’s not about what your business is worth TO THEM. It’s about what it’s worth TO YOU
   - Ransomware: Encrypt your data and expose it publicly… unless you pay.

Average ransomware payment has now climbed to $850,000

43% of cyber attacks target small business

www.cosant.com

Myth: I’m too small to be a cybersecurity target

3. They want your customers, or your suppliers
    - Business Email Compromise: Capture access to email; leverage the access for fraud.

Trick you or your employees to wire $ to a nefarious account

Trick you to pay suppliers to a nefarious account

Trick you or your employees to buy and send gift cards

Redirect your customers to pay invoices to a nefarious account

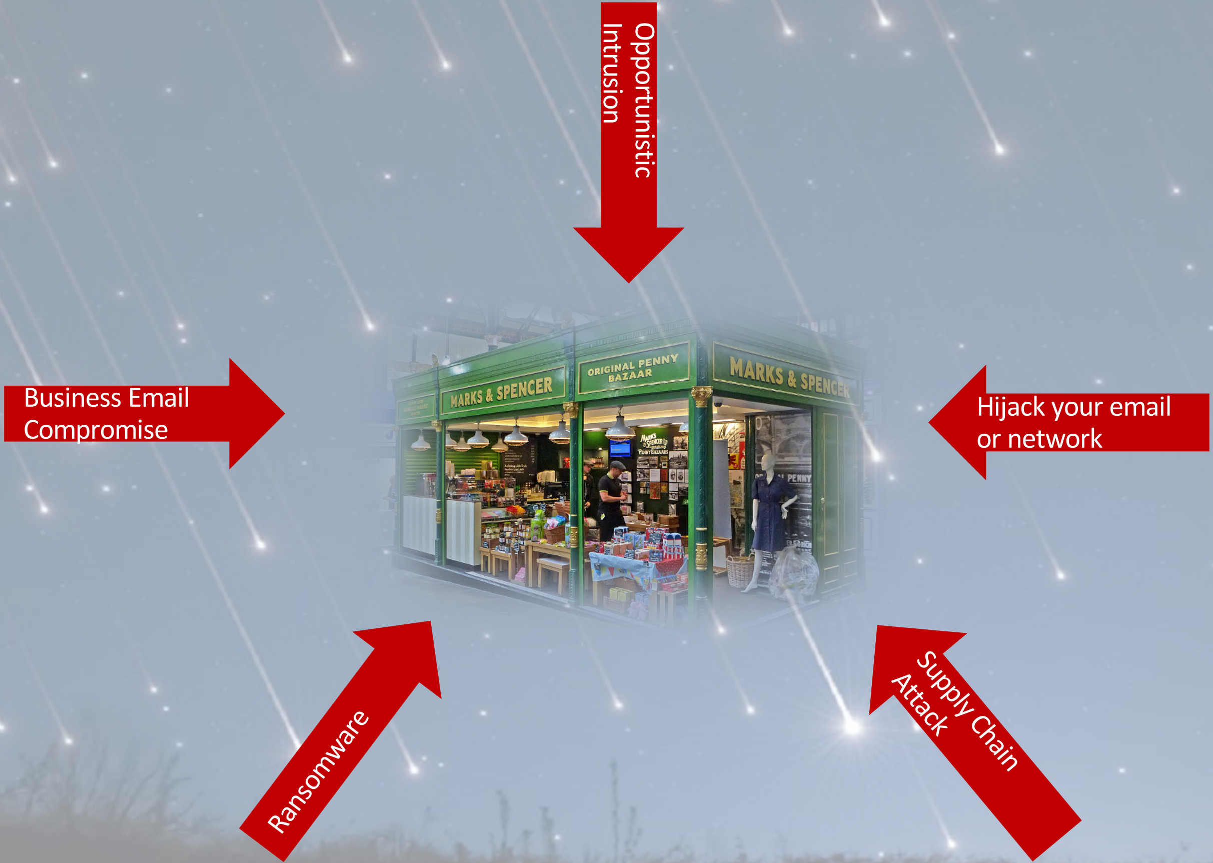
Myth: I’m too small to be a cybersecurity target

4. They use you as an entry point to your customers
   - You’re a means to an end. If you have privileged access to your customers networks, you are THEIR vulnerability.

Myth: I’m too small to be a cybersecurity target

4. What are you really worth to a cyber criminal?
   - Financial assets
   - Personally identifiable information records
   - Personal health information records
   - Financial records
   - What access do you have, to whom?

Small and Medium Business Vulnerability



Opportunistic Intrusion

Business Email Compromise

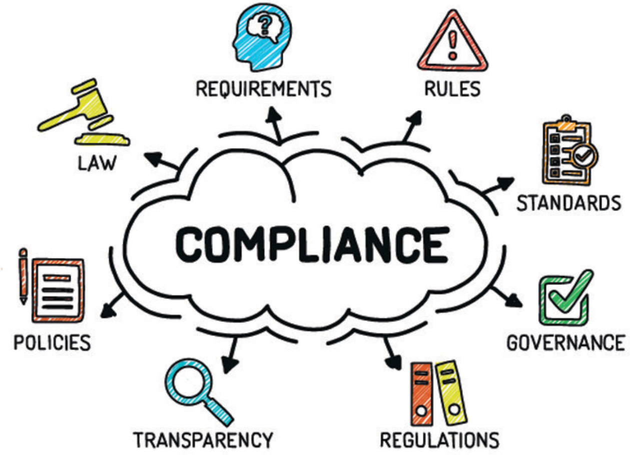
Hijack your email or network

Ransomware

Supply Chain Attack

Beware of incoming Compliance Regulations

- Enterprise companies, Government and insurance are passing along security requirements at an accelerating pace?
  - Do you sales people get security questionnaires?
  - HIPAA, PCI, SOC 2, GDPR, CCPA, CMMC, more… are coming



What can we do?

- Start by LOCKING YOUR FRONT DOOR
  1. Turn on Multi-Factor-Authentication
  2. Use a password manager tool
  3. Change default passwords
  4. Backup your data
  5. Encrypt your notebooks
  6. Train yourself and your staff
  7. Consult your IT team (internal or external)
- Plan ahead
  - What are your biggest risks?
  - What will you do WHEN you have a breach?
  - Engage a security consultant

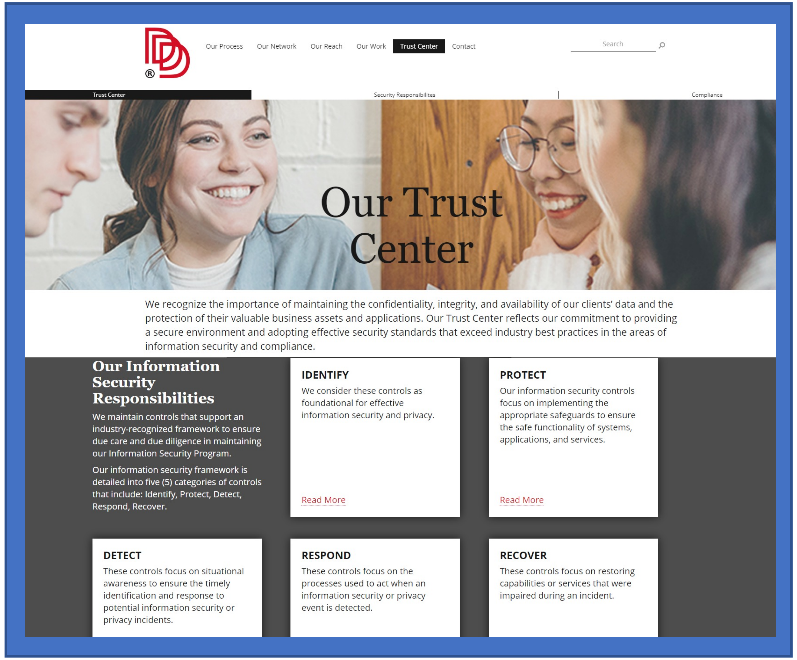
But I Have Cyber Insurance…

- Many cyber insurance policies exclude social engineering attacks
- Most attacks are Social Engineering

- Social Engineering: Phishing, Smishing, Fraud
- Some cyber insurance policies exclude “unauthorized software installation”
- Check your policies for exclusions and clauses

And Don’t forget about Security as Differentiation

- People buy from people they like and TRUST
- Make it easier to buy from you
- If you’re competitors are secure and you’re not… you’ll lose
- Vice-versa
- Accelerate your sales team’s security responses



Our Trust Center

We recognize the importance of maintaining the confidentiality, integrity, and availability of our clients’ data and the protection of their valuable business assets and applications. Our Trust Center reflects our commitment to providing a secure environment and adopting effective security standards that exceed industry best practices in the areas of information security and compliance.

Our Information Security Responsibilities

We maintain controls that support an industry-recognized framework to ensure due care and due diligence in maintaining our Information Security Program.

Our information security framework is detailed into five (5) categories of controls that include: Identify, Protect, Detect, Respond, Recover.

IDENTIFY

We consider these controls as foundational for effective information security and privacy.

Read More

PROTECT

Our information security controls focus on implementing the appropriate safeguards to ensure the safe functionality of systems, applications, and services.

Read More

DETECT

These controls focus on situational awareness to ensure the timely identification and response to potential information security or privacy incidents.

RESPOND

These controls focus on the processes used to act when an information security or privacy event is detected.

RECOVER

These controls focus on restoring capabilities or services that were impaired during an incident.

About Cosant Cyber Security

A vendor-neutral security consultant that helps successful clients who are concerned about compliance and regulatory requirements passed onto them by their customers.

We help clients reduce anxiety about exposing stakeholders to security incidents, reducing the risk to their brand, reputation and income.

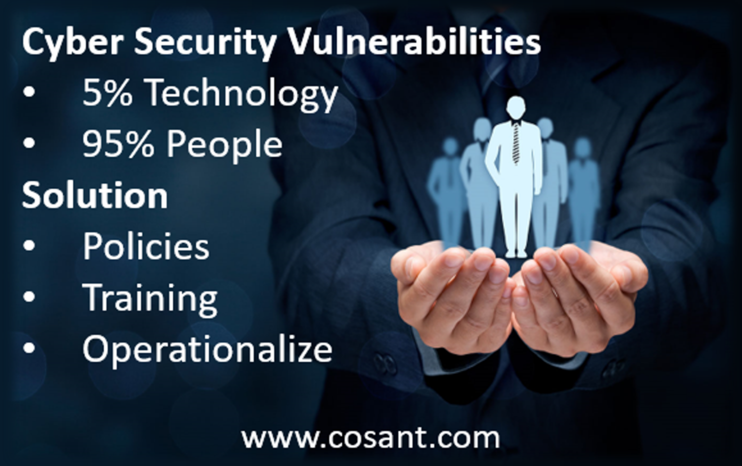
Our 4-step security process:

1. Assess Vulnerabilities and Gaps
2. Build the Security and Resiliency Plan
3. Lead or co-lead plan Execution
4. Maintenance

COSANT
CYBER SECURITY

1st – Identify Vulnerabilities

- Ransomware
- Phishing
- Employees
- Website
- Bank Account & Funds Transfer



Cyber Security Vulnerabilities

- 5% Technology
- 95% People

Solution

- Policies
- Training
- Operationalize

www.cosant.com

2nd – Mitigate Risk

- Risk:

Likelihood of occurrence * Impact of occurrence

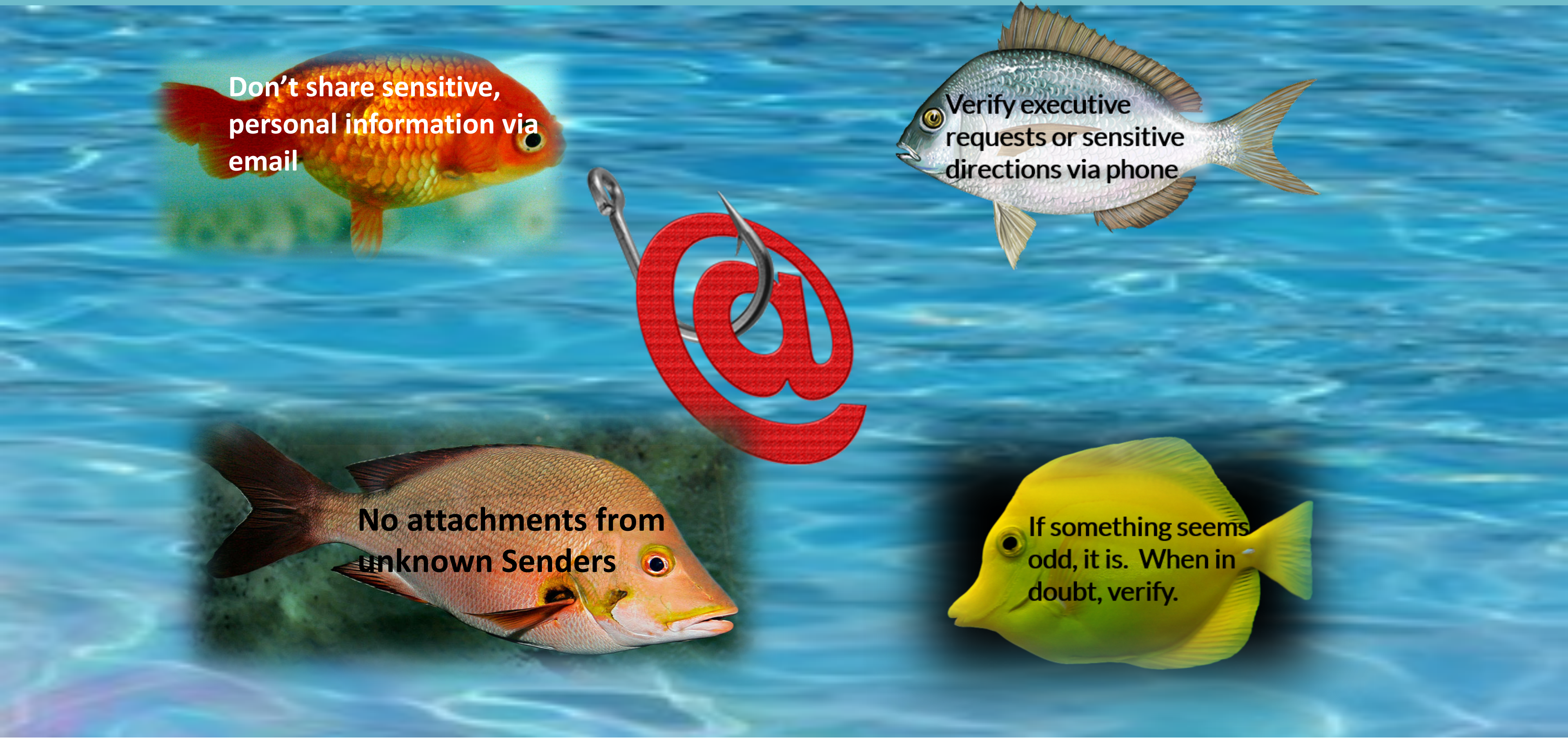
- Return on Security Investment:

Impact of occurrence/cost to remediate

REDUCE
TRANSFER
RISK
ACCEPT
AVOID

There are several Low/No-Cost opportunities to reduce your risk.

Employee Training



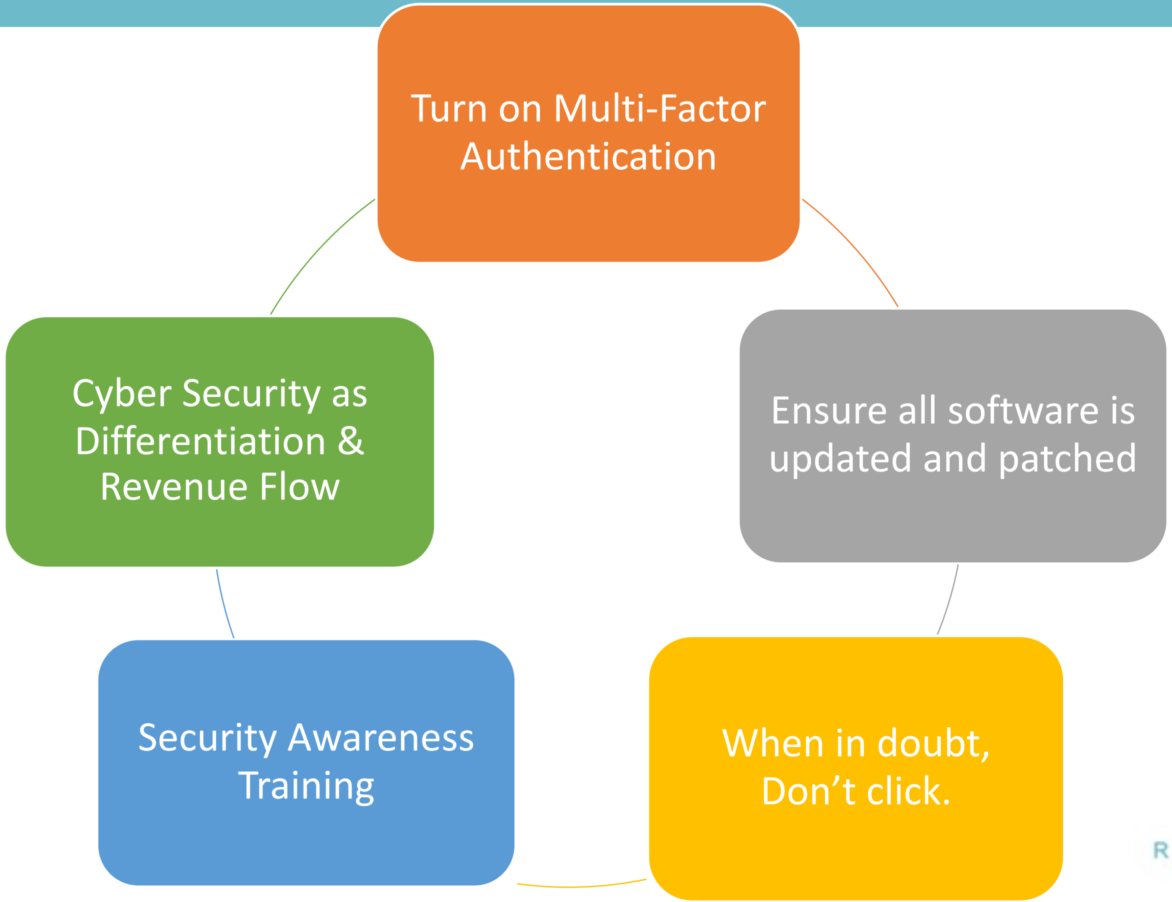
Don’t share sensitive, personal information via email

Verify executive requests or sensitive directions via phone

No attachments from unknown Senders

If something seems odd, it is. When in doubt, verify.

Don’t miss the 5 take-aways



Turn on Multi-Factor Authentication

Ensure all software is updated and patched

When in doubt, Don’t click.

Security Awareness Training

Cyber Security as Differentiation & Revenue Flow

RETURN STRONGER

Our Gift For You…..

1. A top-line “Cost of Incident” estimate using the online calculator we shared before.
   - What is your risk?

2. A dark-web scan of your email address.
   - Are your credentials in the dark?

Text me at 480-678-7778

- Name, Email address, # of customer records, data type (financial, Health, personal)