ARIZONA SMALL BUSINESS BOOT CAMP & COLLECTIVE

RESPOND → PLAN → RETURN STRONGER

COSANT CYBER SECURITY

5 Must Have Cyber Security Tips for SMBs

PRESENTED BY

Mark Kirstein

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

Current Landscape

1. Covid
2. Election
3. Civil unrest
4. Economic Weakness

Why is Cyber Security Relevant Now?

- Cyber Criminals Thrive and manipulate Uncertainty
- Phishing Threats Target Current Mindsets
  - “Covid”, “Election”, “Unemployment”, “Income”, “Holidays”, …
- Regulations and Compliance are Trickling Down from Large Companies
  - Are you Business to Business (B2B)?
  - Do you Touch Personally Identifiable Information (Business to Consumer- B2C)?
- Huge percentage of economic activity aligns with the holidays
  - 2019 US holiday retail sales: over $1.1 trillion
  - Consumers spend 57% of their money in online stores

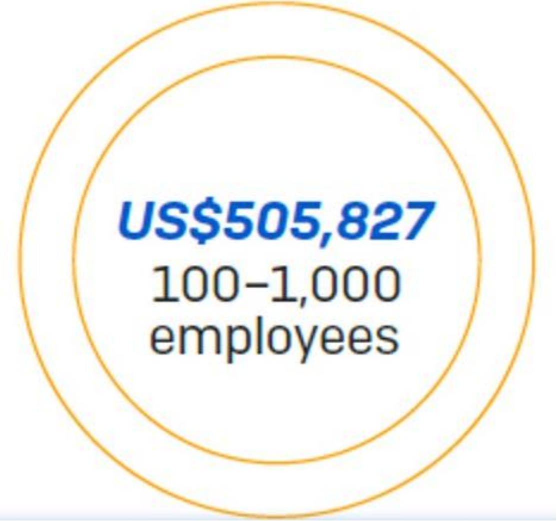
Why think about Cyber Security, now?

1. Reduce likelihood and impact of a security incident

2. Increase Differentiation & Accelerate Revenue

What will a Security Incident Cost?

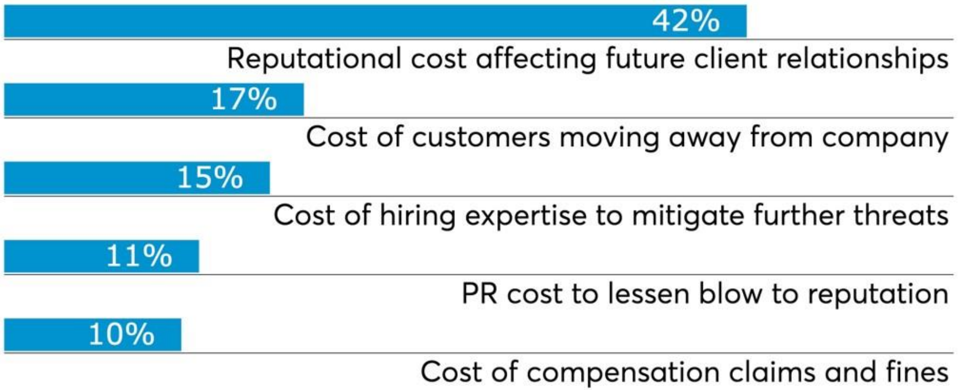
Average Cost to Remediate a Ransomware Attack



Source: The State of Ransomware 2020- Sophos Whitepaper, May 2020

What'll it cost you?

The top costs of a company data breach, according to industry accountants.

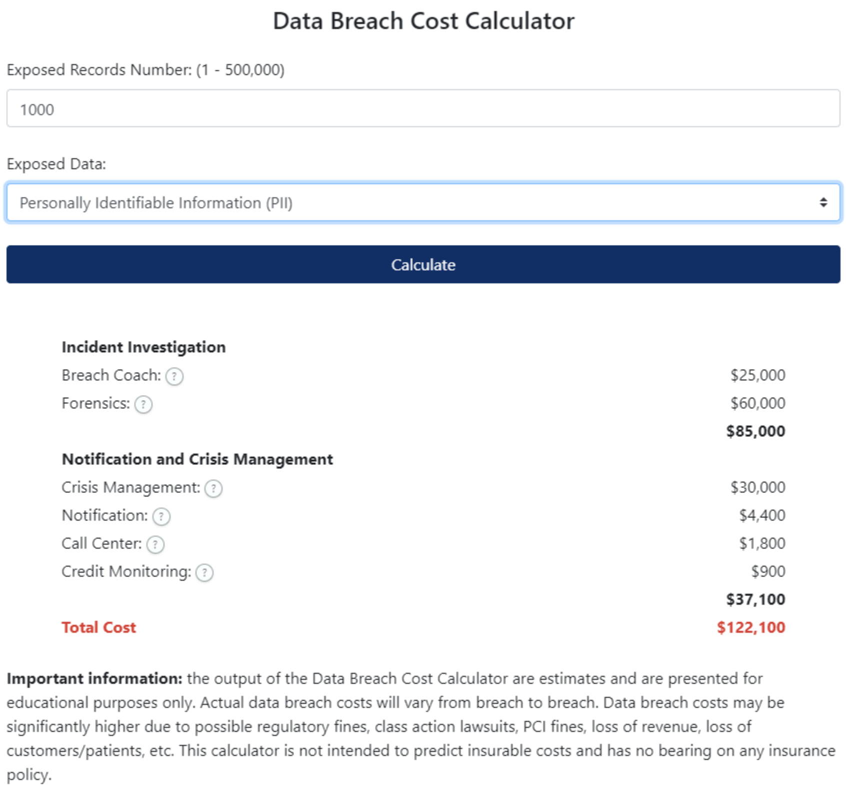


Source: BlackLine

Security Cost Estimate

1,000 Records

PII



Data Breach Cost Calculator

Exposed Records Number: (1 - 500,000)

1000

Exposed Data:

Personally Identifiable Information (PII)

Incident Investigation	
Breach Coach: ?	$25,000
Forensics: ?	$60,000
	$85,000
Notification and Crisis Management	
Crisis Management: ?	$30,000
Notification: ?	$4,400
Call Center: ?	$1,800
Credit Monitoring: ?	$900
	$37,100
Total Cost	**$122,100**

Important information: the output of the Data Breach Cost Calculator are estimates and are presented for educational purposes only. Actual data breach costs will vary from breach to breach. Data breach costs may be significantly higher due to possible regulatory fines, class action lawsuits, PCI fines, loss of revenue, loss of customers/patients, etc. This calculator is not intended to predict insurable costs and has no bearing on any insurance policy.

But I Have Cyber Insurance…

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

- Social Engineering: Phishing, Smishing, Fraud

At Least Keep Your Doors Locked

FBI reported a 300% increase in reported cybercrimes since Covid19

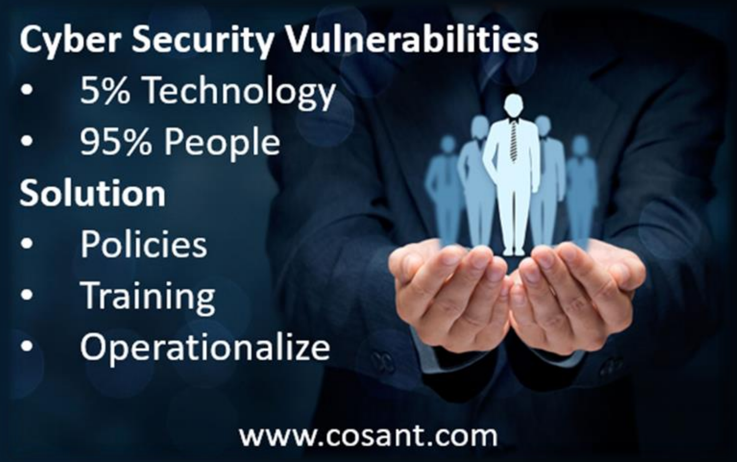
www.cosant.com

A Few Key Tips can Reduce Your Exposure

… with minimum or low investment

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

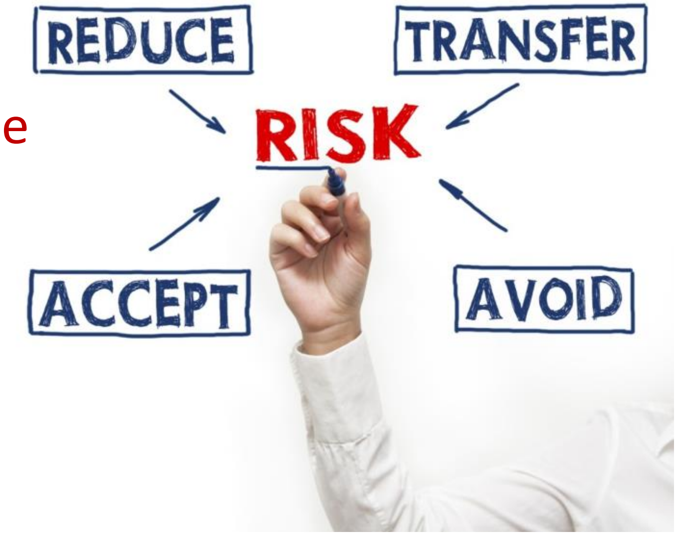
2nd – Mitigate Risk

- Risk:

Likelihood of occurrence * Impact of occurrence

- Return on Security Investment:

Impact of occurrence/cost to remediate



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

Ransomware

- Biggest Threat: Destroying Essential Data
  - Backup Data – Cloud Storage, Local Storage, Backup Applications
  - Enable Multi-Factor Authentication

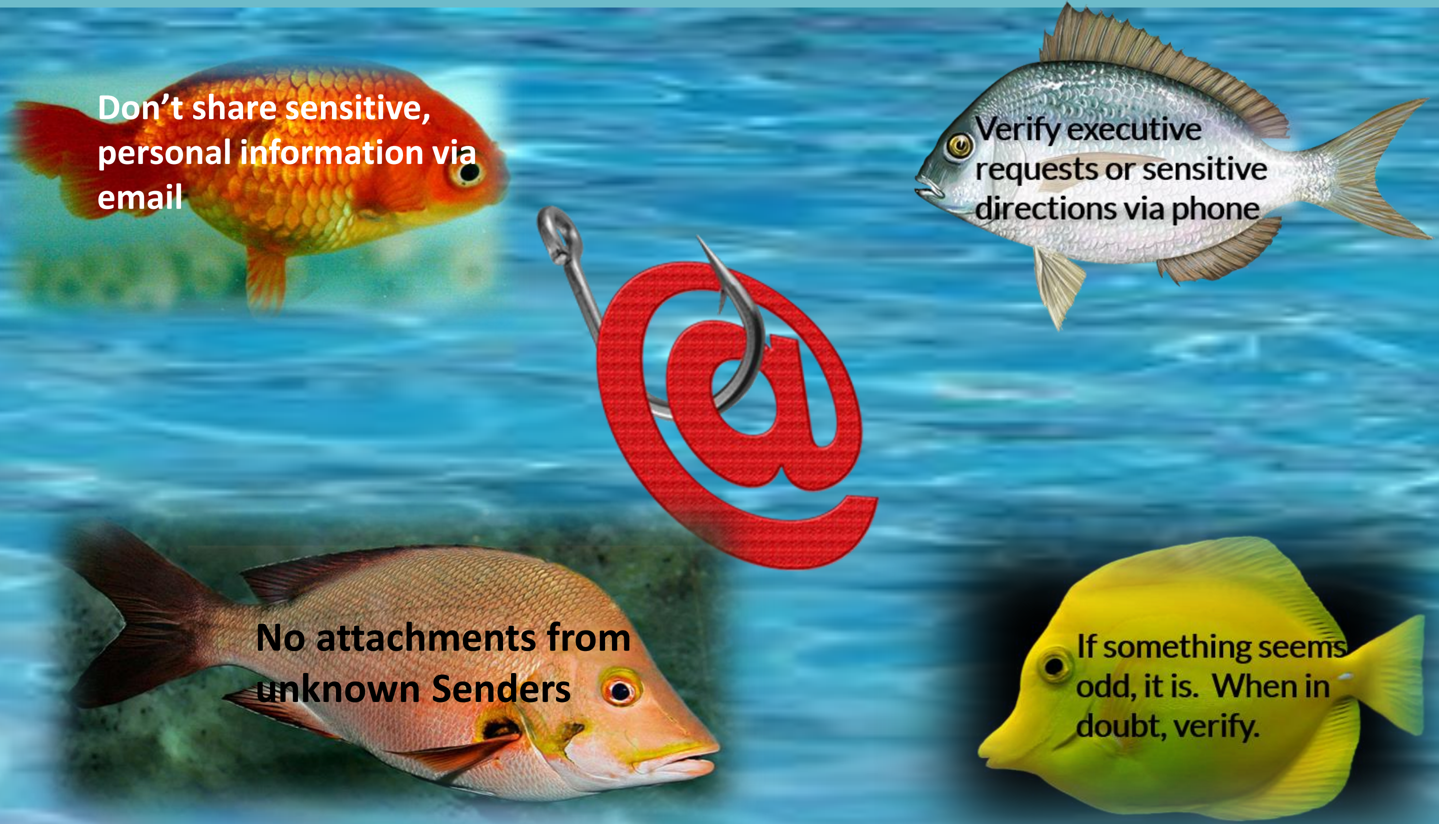
Any of these relevant?

✓Local Data: Encrypt Windows | Mac & Back Up Windows | Mac
✓CRM: SalesForce Authenticator
✓Email: Microsoft Authenticator
✓Cloud Storage: DUO Authenticator

Secure Employees

- Technology
  - Setup Data Access Restrictions: Role-Based Access
  - Use Password Manager: LastPass
  - DNS Blocker
  - Ad Blocker
  - Anti-Virus
  - Recurring Software Updates
- Policy
  - Require Generated Security Passwords
  - No saving passwords in the Web Browser
- Training

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.

Phishing

- Set up a Security Gateway
- Recurring Phishing Tests on Employees
- Set Up DMARC

Website

- Make sure your web page team is security conscious
- Ask them about
  - SSL/TLS Encryption
  - CMS Vulnerabilities (Content Management System, such as WordPress)
  - Regulatory Compliance (GDPR, PCI)

Bank Accounts & Fund Transfers

- Enable Multi-Factor Authentication for Banking
- Use Bank Tokenized Keyfob
- Require Call-back prior to Transfer
- 2nd Signature for Transfers above a threshold

3rd - Differentiate & Accelerate Revenue

First a few questions for you:

1.) Who is in business to make a **profit**?
2.) Is **margin** important for you?
3.) What about driving top line **revenue**?

Now…
A.) Who wants to add friction and obstacles that slow your clients down?
B.) Anybody in favor of elongating your customer's sales cycle?
C.) Should we make the cost of sales MORE expensive?

Umm, AND why is the information security nerd talking about driving sales, margin and profitability…?

A problem that's only getting bigger, more complex and more expensive to solve…

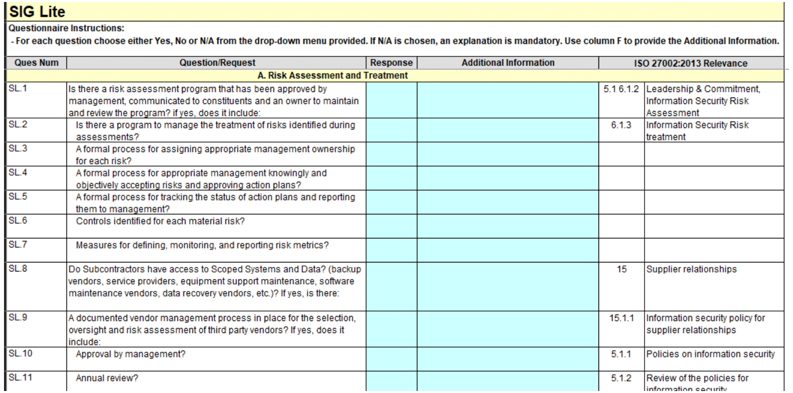
If you haven't observed it yet, you will soon …

Most common story:

- Sales team works hard to close
- Pricing and terms negotiated
- Contractual process includes one or multiple

- Vendor Risk Assessments
- 3rd Party Risk Assessments
- Information Security Questionnaires
- Data Security Questionnaires
- Data Security Requirements
- Contractual provisions for data security and privacy
- Privacy provisions
- Personal information
- GDPR clause
- CCPA clause

Let's look at a SIG Lite – only 300 questions



SIG Lite

Questionnaire Instructions:

- For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use column F to provide the Additional Information.

Ques Num	Question/Request	Response	Additional Information	ISO 27002:2013 Relevance	
	A. Risk Assessment and Treatment				
SL.1	Is there a risk assessment program that has been approved by management, communicated to constituents and an owner to maintain and review the program? if yes, does it include:			5.1 6.1.2	Leadership & Commitment, Information Security Risk Assessment
SL.2	Is there a program to manage the treatment of risks identified during assessments?			6.1.3	Information Security Risk treatment
SL.3	A formal process for assigning appropriate management ownership for each risk?				
SL.4	A formal process for appropriate management knowingly and objectively accepting risks and approving action plans?				
SL.5	A formal process for tracking the status of action plans and reporting them to management?				
SL.6	Controls identified for each material risk?				
SL.7	Measures for defining, monitoring, and reporting risk metrics?				
SL.8	Do Subcontractors have access to Scoped Systems and Data? (backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, etc.)? If yes, is there:			15	Supplier relationships
SL.9	A documented vendor management process in place for the selection, oversight and risk assessment of third party vendors? If yes, does it include:			15.1.1	Information security policy for supplier relationships
SL.10	Approval by management?			5.1.1	Policies on information security
SL.11	Annual review?			5.1.2	Review of the policies for information security

Dealing with Security Questionnaires and Regulations

- Sales team herds these cats:
  - IT
  - HR
  - Legal
  - Outsourced partner
  - Others

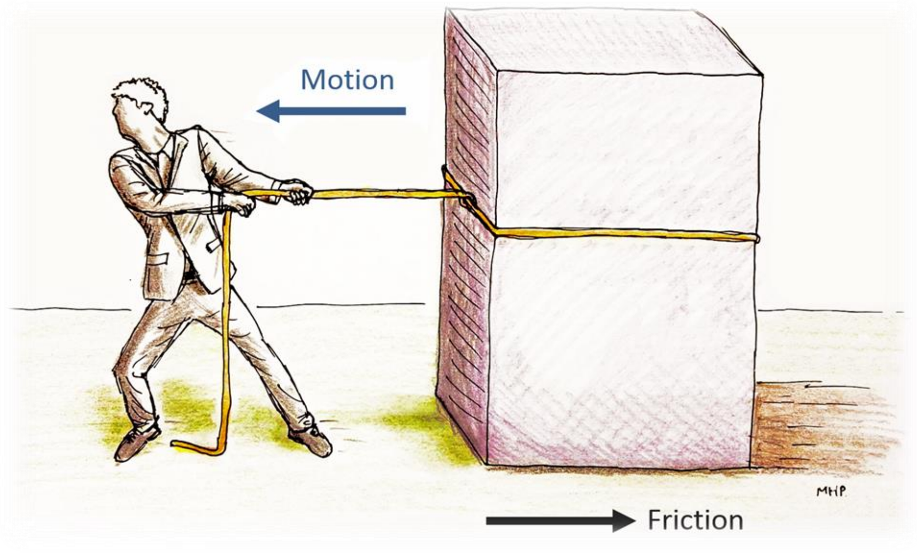
- IT is lost or misrepresenting the organization
- The questionnaires are kicked back for a multitude of reasons
- Meetings between IT and the prospect's risk & compliance people

The sales process stalls while all this chaos is addressed

It’s what we call, FRICTION in the Sales Process

With these effects

- Slows Revenue Recognition- Longer Sales Cycles
- Inefficiency in the Sales Process
  - Reduces Revenue
  - Increases Costs
- Reduces Motivation



What Can We do About it?

DIY

1. Centralize your Response to Security Questionnaires
   - Sales Ops, Accounting

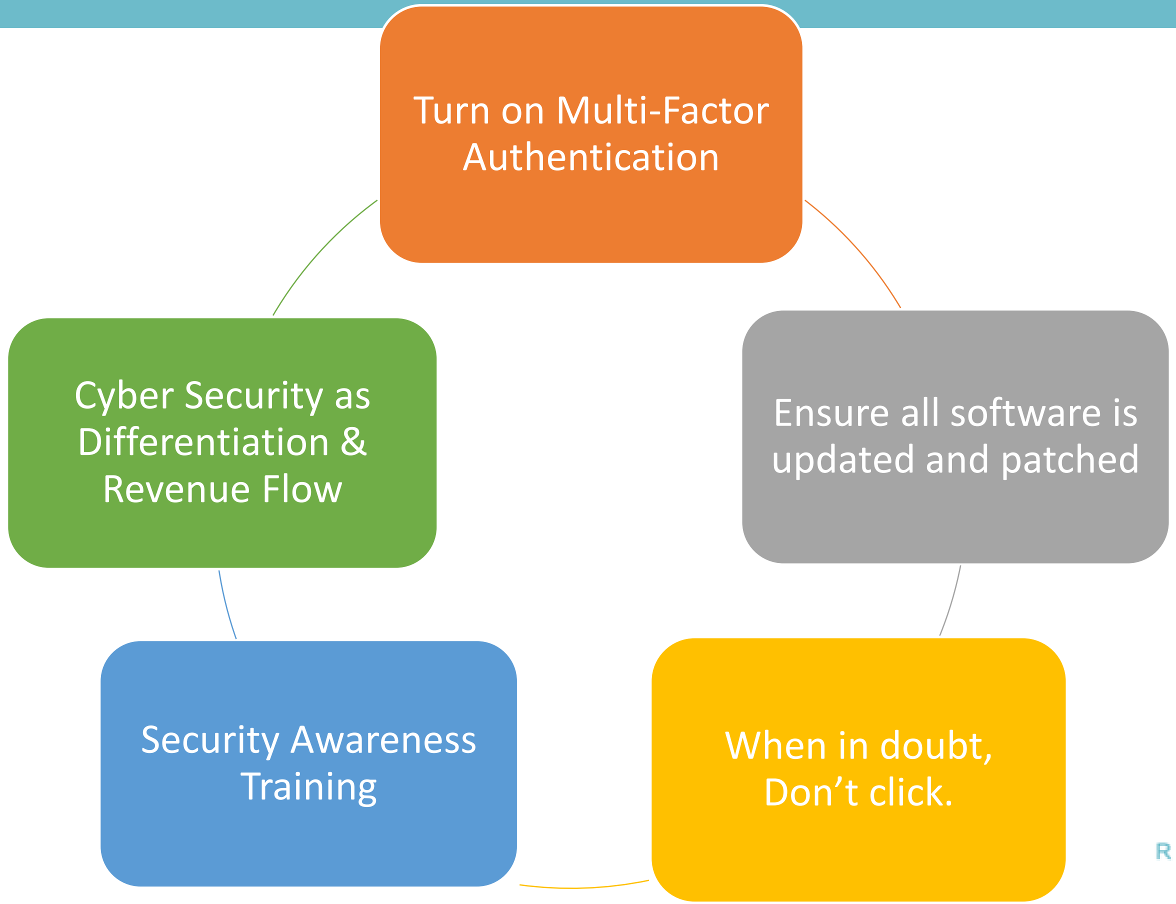
DIY

2. Keep a Library of Security Questions and Responses
   - Categorized and Reusable

We Help

3. Automate Questionnaire Response with Software

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)

My Contact Information

Mark Kirstein

VP, Customer Success
Cosant Cyber Security
480-678-7778
Mark@Cosant.com

COSANT
CYBER SECURITY

It’s about your Risk and Reputation,
Not Your Technology ®