Protecting Your Entity From Fraud

League of California Cities
Municipal Finance Institute
December 11, 2019

When poll is active, respond at PollEv.com/richardlee897

Has your entity been affected by cyber fraud in the past 12 months?

Yes

No

Total Results: 0
Has your entity been affected by cyber fraud in the past 12 months?

Yes

No
Hi,

We are currently in the process of registering as a vendor of City of San Mateo and we would like to know if you do make ACH/EFT payments as our preferred method of invoice payment. If you do make payments via this mode, kindly forward me an Enrollment Form.

Regards,
Taking a closer look

Kinsley Power Systems
www.kinsley-group.com
Welcome to the Kinsley Group: a top energy solutions supplier with a 50-year legacy of sales, rental and service of quality energy systems.

Email Recipient & Greeting

To Richard Lee

Flag for follow up.
You forwarded this message on 11/20/2019 8:35 AM.

Hi,
Cyber Security

10 Keys To Keeping Your Company Safe

SECURITY TRIAD

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

INFORMATION SECURITY

NO TRESPASSING
How Does a Data Breach Occur

(from = MGO Technology Group)

breach #1

(Phishing)

breach #2

(Missing Laptop)

breach #3

(Allow others to access your information)

breach #4

(Inadvertent disclosure - accidents happen)
< breach #5 >
{(Weak passwords)}

< breach #6 >
{(Vendors access)}

< breach #7 >
{(Ransomware)}

< breach #8 >
{(Misconfigured network)}

<What is BEC?>

{(Business Email Compromise or Man-in-the-Email Scam)}
<Version 1: The Bogus Invoice Scheme>

{Attacks pretend to be the suppliers requesting fund transfers for payments to an account owned by fraudsters}

<Version 2: CEO Fraud>

{Attacks pose as the company CEO or any executive and send an email to employees in finance, requesting them to transfer money to the account they control}
<Version 3: Account Compromise>

{(An executive or employee’s email account is hacked and used to request invoice payments to vendors listed in their email contacts. Payments are then sent to fraudulent bank accounts)}

<Version 4: Attorney Impersonation>

{(Attackers pretend to be a lawyer or someone from the law firm supposedly in charge of crucial and confidential matters. Normally, such bogus requests are done through email or phone, and during the end of the business day)}
<Version 5: Data Theft>

Employees under HR and bookkeeping are targeted to obtain personally identifiable information (PII) or tax statements of employees and executives. Such data can be used for future attacks.
Two-thirds of SMBs have suffered a cyber attack in the past 12 months.

{So much for the idea that small business = under the radar}
The average cost of an attack is nearly $3 million.

Downtime accounts for slightly more than half the price tag for the average attack.

92.4% of malware is delivered via email.

A phishing email related to billing or an invoice is the most common.
<4 out of 5 SMBs report malware has evaded their antivirus>

{for SMB the most cost effective answer is a Managed Service Provider}

<3 out of 4 SMBs say they don’t have sufficient personnel to address IT security>

{who ya going to call – Ghost Busters}
<Security Tips>

1. Security awareness
2. Back up your data daily
3. Patch software immediately
4. Limit the number of people who can install software
5. Use a reputable antivirus software

{{ from = MGO Technology Group }}
Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid.
Ransomware costs businesses more than $75 billion per year.

A new organization will fall victim to ransomware every 14 seconds in 2019.
34% of businesses hit with malware took a week or more to regain access to their data.

FBI Issued a PSA
High-Impact
Ransomware Attacks
Threaten U.S. Businesses And Organizations
Cyber & Information Security Roadmap
Addressing Business Risks and Providing Peace of Mind

1. Conduct internal and external threat assessments.
2. Bolster access controls.
3. Assess 3rd PartyVendor Risk, ensure they protect your information.
4. Ensure 24 x 7 x 365 monitoring of your network with advanced Operation Security (NOC/SOC).
5. Establish program leadership or vCISO.
7. Security Awareness is everyone’s responsibility.
9. Develop and test a Business Continuity Plan (BCP) and Disaster Recovery (DR) plan.
10. Create an Incident Response Plan.
Available 24 X 7
Let’s Talk.

Karl Kispert, Managing Director, MGO Technology Group, LLC
kkispert@mgocpa.com
212.441.3167 (o)
973.229.5566 (c)