TML
INTERGOVERNMENTAL RISK POOL

The Cybersecurity Pandemic

To partner with local governments so that Texas communities are STRONGER TOGETHER

It won't happen to us…

June 14, 2024

The City of Cleveland publicly acknowledged for the first time on Friday that a ransomware attack is what's behind the closing of City Hall and the stoppage of some city services this week.

June 13, 2024

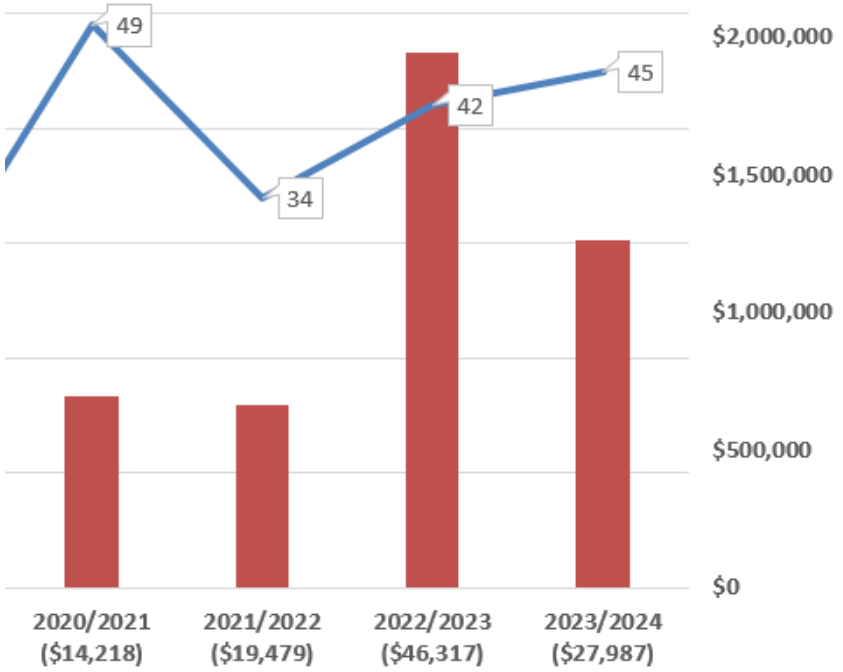
Alarm in Texas as 23 towns hit by 'coordinated' ransomware attack

April 22, 2024

Jackson County's ransomware attack is just the latest cybercrime to target local governments

Claims – What are Our Members Seeing

- 261 claims reported since 2016
- $5.4M incurred (over $20K average per claim reported)
  - 121 in last 3 years
  - $3.87M in last 2 ½ years



Claims – What are Our Members Seeing

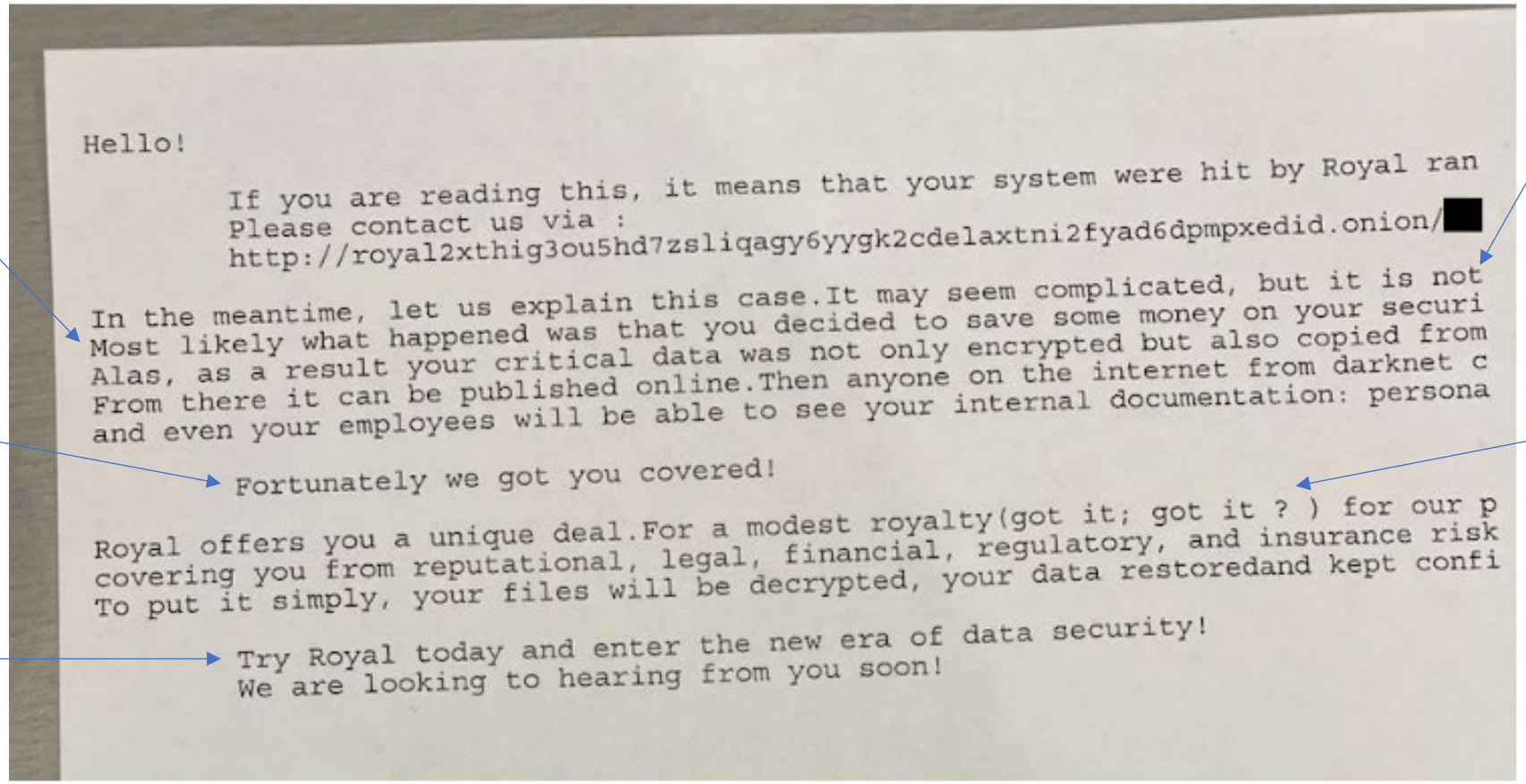
- Ransomware
  - Encryption of Data
  - Double Extortion
- Fraudulent Instruction/EFT
  - Business Email Compromise on Member's side
  - Business Email Compromise on Vendor side

Royal Pain in the…

So not our fault!

So helpful!

So what are you waiting for?!



Hello!

If you are reading this, it means that your system were hit by Royal ran
Please contact us via :
http://royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid.onion/[redacted]

In the meantime, let us explain this case.It may seem complicated, but it is not
Most likely what happened was that you decided to save some money on your securi
Alas, as a result your critical data was not only encrypted but also copied from
From there it can be published online.Then anyone on the internet from darknet c
and even your employees will be able to see your internal documentation: persona

Fortunately we got you covered!

Royal offers you a unique deal.For a modest royalty(got it; got it ?) for our p
covering you from reputational, legal, financial, regulatory, and insurance risk
To put it simply, your files will be decrypted, your data restoredand kept confi

Try Royal today and enter the new era of data security!
We are looking to hearing from you soon!

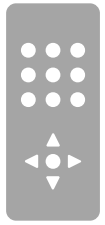
So easy!

So funny!

Royal Ransomware Attack Vectors

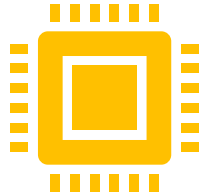
Phishing – 66.7%

Victims unknowingly install malware after receiving email with malicious PDF



Remote Desktop Protocol – 13.3%

Unsecure RDP for initial access



Public Facing Applications and Brokers – 20%

Exploiting those applications or leveraging brokers for harvesting VPN credentials form stealer logs

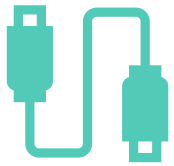
** CISA #StopRansomware: Royal Ransomware Update*

How Do I Protect Against Ransomware?

- Train Your Staff
- Use Multi-Factor Authentication (MFA)
- Have a Strong Password Policy
- Implement Principal of Least Privilege (PoLP)
- Portable Media Controls
- Patch Systems
- Backup Your Data
- Leverage Available Resources
- Cyber Insurance

Train Employees

Overall cyber awareness



Physical device security, physical premises security, public WiFi, USB

Onboarding/Offboarding

Simulated phishing campaigns

Phishing Red Flags

Urgent requests, action to avoid a negative consequence	Bad grammar or misspelled words	Emails sent at unusual times or unsolicited	Email address from suspicious domain/doesn't match vendor domain
Hyperlinks to a different domain or misspelled	Suspicious attachments	You are one of multiple recipients	Something too good to be true
Any unsolicited request to log in/change user credentials	Any request to send money, change a money transfer procedure	No legitimate security or administrative person will ever ask for a password or MFA One Time Passcode	Never approve an unsolicited MFA authentication request

What is Multi-Factor Authentication (MFA)?

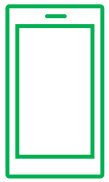
Requires two or more of the below “factors” to access a resource

Something you Know

Username & Password

Pin

Security Questions



Something you Have

Device (smart phone, workstation)

Hard Token (USB device)

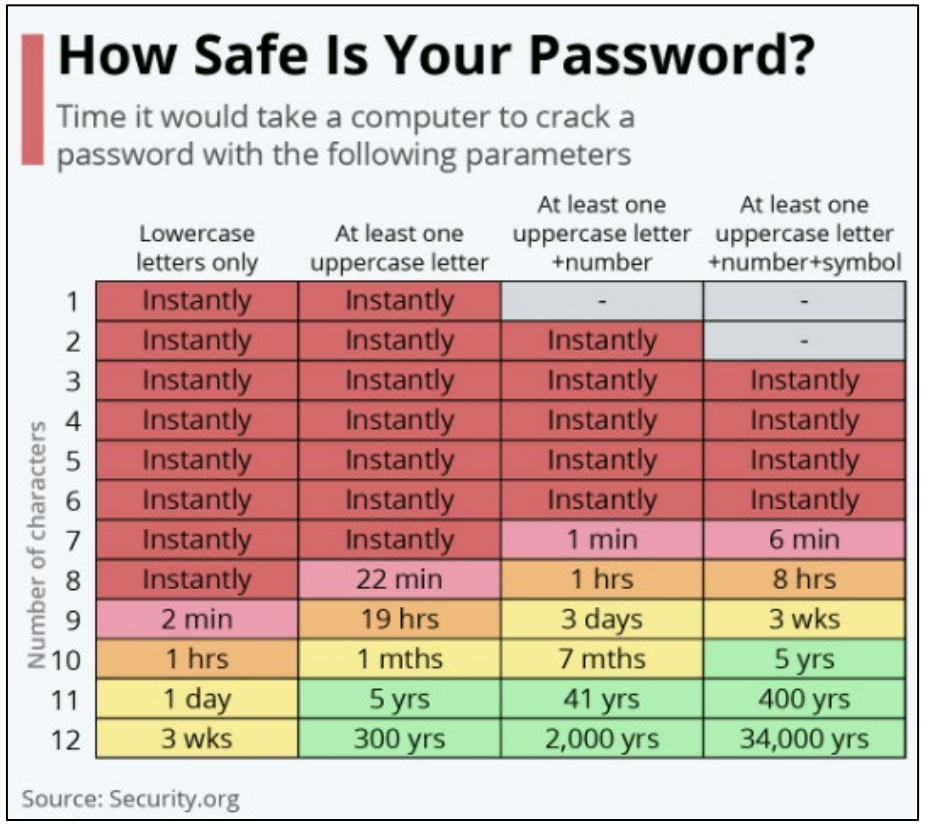
Something you Are

Biometrics (Face ID, Fingerprint)

> “Implementing MFA can make you 99% less likely to get hacked, according to Microsoft.”

Use Strong Passwords

- Do everything you can to avoid using the same password in more than one place.
  - Password reuse accounts for 82% of breaches*
- Random alphanumeric strings, the longer the better (12+ ideally)
  - Brute force can still crack any password, but the more complex the longer it will take to be breached
- Password managers are recommended
  - Encrypted
  - Generate random complex passwords
  - Can autofill or copy/paste
- Saving login credentials to your browser is **NOT** encrypted. Malware can harvest this data.



How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

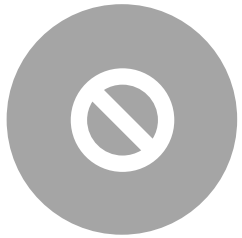
Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

2022 Verizon Data Breach Report

Principle of Least Privilege

MINIMIZES ATTACK SURFACE



CAN STOP SPREAD OF MALWARE

ACCOUNT COMPROMISE OF OVER-PRIVILEGED USER

AUDIT – ELIMINATE UNNECESSARY LOCAL ADMIN PRIVILEGES

SEPARATE ADMIN ACCOUNTS FROM STANDARD ACCOUNTS – DIGITAL VAULT

What is Portable Media?

- Some require being wired to transfer data:
  - External Hard Drives
  - USB drives
  - CD/DVDs
  - Portable music players
- Some use Wi-fi or Cellular networking:
  - Smart phones
  - Tablets, laptops
  - Gaming devices
  - E-readers

Best Practices for Portable Devices

- Limit the use of removable media and consider banning personal devices
- Create security and acceptable-use policies for portable media devices and educate your employees
- Teach employees to report missing devices IMMEDIATELY
- Consider the costs and benefits of using locked-down, corporate-controlled devices versus “bring your own device” policy
- Only allow access through a VPN connection

Patch Often

- Addresses vulnerabilities in software/applications
- Supports system uptime
- Can maintain compliance standards
- Establish asset management
- Prioritize vulnerabilities

Data Backups

EASY AS 3, 2, 1…

TEST YOUR BACKUPS

DISASTER RECOVERY AND APPLICATION AVAILABILITY

KNOW YOUR RECOVERY POINT OBJECTIVE AND RECOVERY TIME OBJECTIVE

ENCRYPT AND PHYSICALLY PROTECT

Leverage Available Resources

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

- Region 6
  - Offices in Texas:
    - Austin
    - Dallas
    - Houston
    - San Antonio
  - Provide risk mitigation advice, outreach, assessments, inspections, trainings, support and more

- Who is CIS?
  - Community-driven nonprofit
  - Responsible for CIS Controls and CIS Benchmarks – both are recognized best practices for securing IT systems and data
  - CIS Risk Assessment Method
    - Provides instructions, examples, templates, and exercises
    - Runs against the CIS Controls and best practices

- CIS Securesuite
  - Free to SLTT organizations
  - Access to cyber tools
  - Compare your configuration against best practices
  - Track your implementation of CIS Controls with self-assessment tool
  - Customize your configuration policies

More info: https://www.cisecurity.org/

Partnership

CISA focuses on the cybersecurity of all critical infrastructure within the United States (including election offices).

MS-ISAC® Multi-State Information Sharing & Analysis Center®

The MS-ISAC is a trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

Elections Infrastructure ISAC®

The EI-ISAC supports the rapidly changing cybersecurity needs of U.S. SLTT election offices.

CIS

CIS is home to the MS-ISAC and the EI-ISAC

MS-ISAC

The Multi-State Information Sharing and Analysis Center (MS-ISAC) mission is to improve the cybersecurity poster of U.S. State, Local, Tribal, and Territorial (SLTT) **government organizations** through coordination, collaboration, cooperation, and increased communication.

https://www.cisecurity.org/ms-isac

MS-ISAC

NO COST Services:

- Security Operations Center (SOC) – 24x7x365 monitors, analyzes, and responds to cyber incidents targeting SLTT entities.
- Cyber Incident Response Team (CIRT) – provides SLTT org's with malware analysis, forensics, and incident response. They also offer external vulnerability assessments after a cyber incident
- Foundational Assessment – 32 question assessment to get your started on evaluating your current cybersecurity posture
- CIS SecureSuite Membership – gives org's access to a collection of resources
- Many more….

EI-ISAC

The Election Infrastructure Information Sharing and Advisory Center (EI-ISAC) works closely with election officials and security and technology personnel to provide the highest standards of election security, including incident response and remediation through their team of cyber experts.

https://www.cisecurity.org/ei-isac

EI-ISAC

The Cybersecurity and Infrastructure Security Agency (CISA) just published a new guide on election security. List of first steps to secure your elections:

- Enable MFA!
- Manage cyber vulnerabilities (sign up for CISA's free cyber hygiene vulnerability scanning)
- Get a no-cost physical security assessment
- Get a dot .gov domain
- Rehearse your incident response plan
- Join the EI-SAC

More info: https://www.cisa.gov/topics/election-security

Cyber Insurance

Know the Terms & Conditions

Panel of providers?

- If not, what are the requirements?
- Pre-breach vs. post-breach

What are the requirements for renewal?

Don’t rely on cyber insurance alone

Cyber Insurance

	Core	Core+
Tower 1 - Limit of Liability*	$500,000	$1,000,000
Data & Network and Media Liability Aggregate Limit of Liability	$500,000	$1,000,000
Retention	$0	$0

Tower 2 - Limit of Liability	$100,000	$250,000
First Party Loss		
Business Interruption Aggregate Sublimit	$20,000	$50,000
Cyber Extortion Loss Aggregate Sublimit	$25,000	$50,000
Data Recovery Costs Aggregate Sublimit	$20,000	$50,000
Reputational Loss Aggregate Sublimit	$5,000	$10,000
Retention (other than Business Interruption)	$0	$5,000
Income Loss Retention under Business Interruption	$5,000	$5,000
Third Party Loss		
Regulatory Defense and Penalities Aggregate Sublimit	$25,000	$75,000
Payment Card Liabilities & Costs Aggregate Sublimit	$10,000	$25,000
Retention	$0	$5,000

Cyber Insurance

eCrime		
Fraudulent Instruction Aggregate Sublimit	$25,000	$50,000
Funds Transfer Aggregate Sublimit	$25,000	$50,000
Telephone Fraud Aggregate Sublimit	$25,000	$50,000
Criminal Reward	$2,500	$2,500
Retention (other than Criminal Reward)	$2,500	$5,000
Retention Criminal Reward	$0	$0

Tower 3 - Limit of Liability	$100,000	$150,000
Breach Breach Response Aggregate Limit of Liability Beazley Response Services	$100,000	$150,000
Retention	$0	$0

EFT Fraud-Fraudulent Instruction Loss

- Annual training to identify social engineering, business email compromise, etc.
- Secondary verification for new vendor in AP system
- Secondary verification for ANY change in payment process initiated by VENDOR
- Secondary verification for ANY change in payment process initiated by EMPLOYEE
- Additional internal approver once verification has been made (per bullets above)
- Next-level supervisor approval before processing ANY funds transfer requests

EFT Fraud-Fraudulent Instruction Loss

[Fraudulent Instruction YouTube Video]

TML Risk Pool Resources

CYBERSECURITY BEST PRACTICES

INFORMATION SECURITY POLICY REVIEW/DEVELOPMENT

INCIDENT RESPONSE PLAN REVIEW

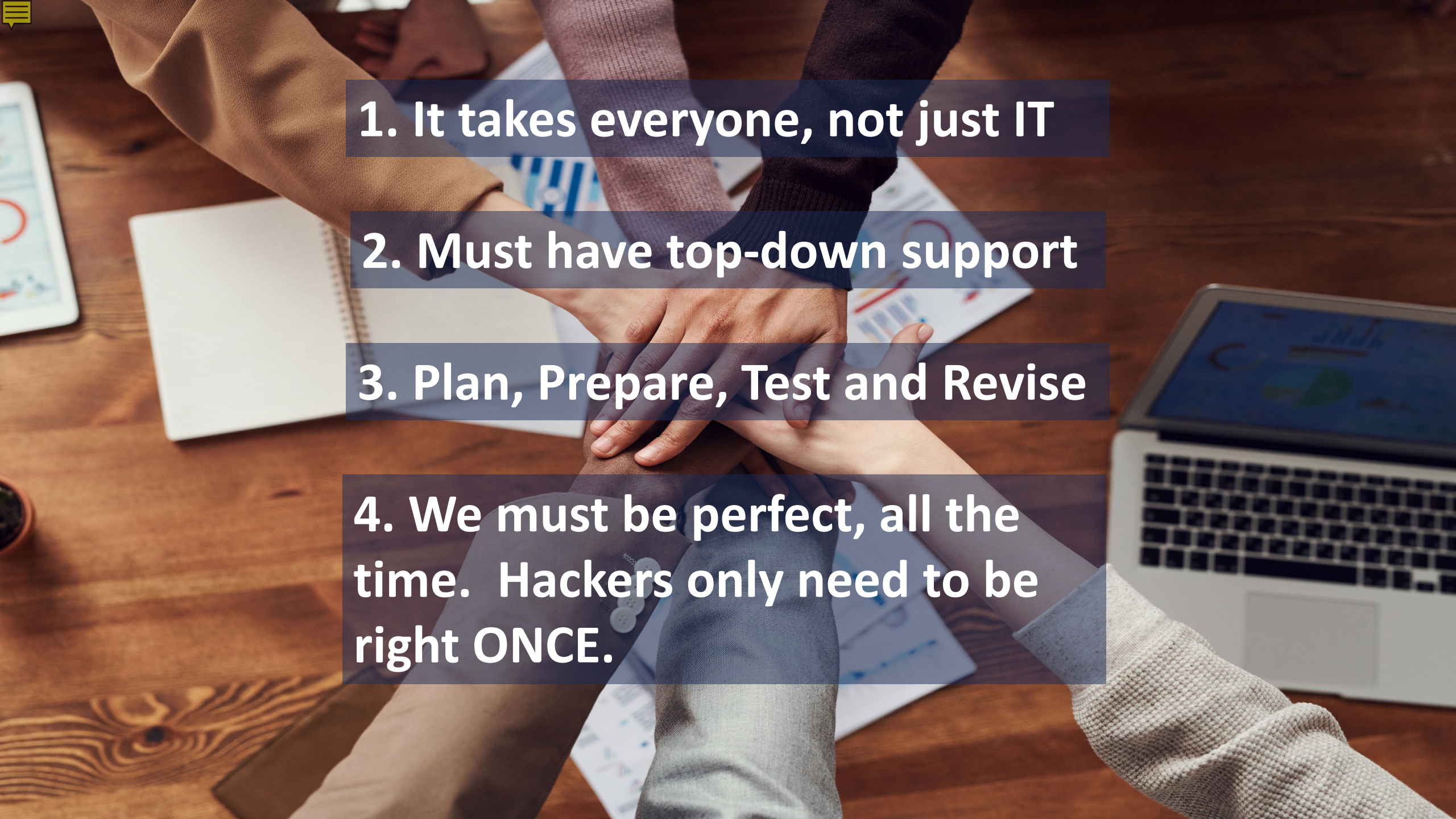
RISK ASSESSMENT ASSISTANCE

TABLETOP CYBERSECURITY EXERCISES

DISASTER RECOVERY PLANNING

CYBERSECURITY TRAINING

INFORMATION SECURITY JOB DESCRIPTIONS


1. It takes everyone, not just IT
2. Must have top-down support
3. Plan, Prepare, Test and Revise
4. We must be perfect, all the time. Hackers only need to be right ONCE.

Questions?

Ryan Burns
Cyber Risk Services Manager
Ph: (512) 491-3427
rburns@tmlirp.org

Mike Bell
Sr. Cybersecurity Advisor
Ph: (512) 491-2305
mike.bell@tmlirp.org