networking

We design and support business networks by project or SPOT Managed.

security

Let us enhance your security posture with policies, auditing or tools.

voip

Empower your phones with lower costs and more functionality.

storage

Explore the benefits of centralized storage and make life easier.

dr/bc

We can keep critical systems, servers, and WAN links more available.

services

Get advanced benefits from hosted services.

What’s New in Cybersecurity

THE FULCRUM GROUP

One Technology Solution: Yours

Presented by
David Johnson
December 10th, 2024

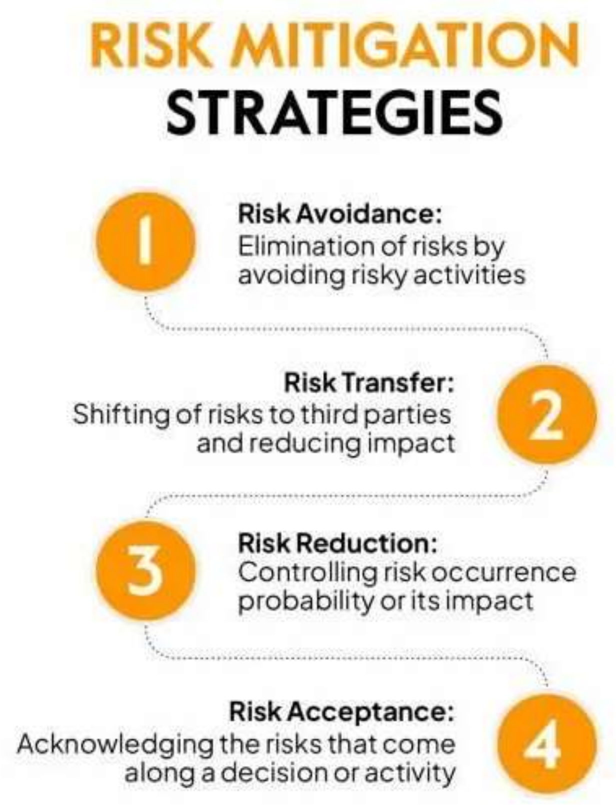
Agenda

- Risk Management Reminder
- What’s Changed in the Last 3 Years
- What it means to be a Cyber Focused CEO
- Yesterday’s Cybersecurity isn’t Enough
- In summary - 5 Things You Can Do NOW

Risk Management At A Glance

- Exit a risky vertical
- Avoid single supply chain areas
- Cash flow management
- High cost of sales markets

- Conduct accounting, legal, IT, compliance risk assessments
- Cross train employees
- Strong supplier relationships
- Competitor market analysis



RISK MITIGATION STRATEGIES

1. **Risk Avoidance:** Elimination of risks by avoiding risky activities
2. **Risk Transfer:** Shifting of risks to third parties and reducing impact
3. **Risk Reduction:** Controlling risk occurrence probability or its impact
4. **Risk Acceptance:** Acknowledging the risks that come along a decision or activity

- Insurance coverages
- Contractual agreements
- Outsourcing
- Leasing equipment

- Make budget decisions
- Keep your business agile
- Positive employee experiences
- Stay informed on regulation changes

Reasonable and Proactive

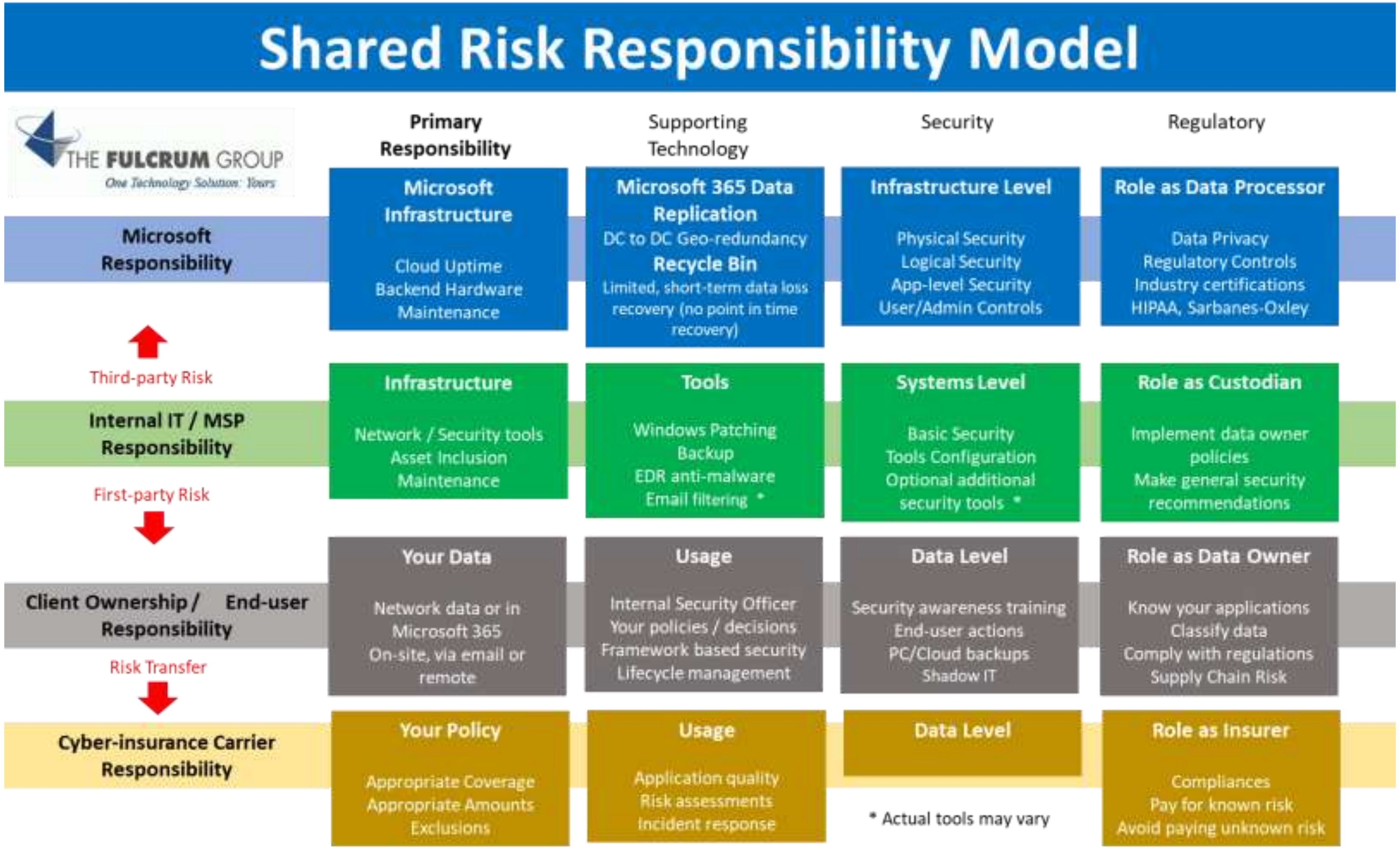
CIS Control 17.2 Establish and Maintain Contact Information for Reporting Security Incidents

Understanding Cyber Risk

- Not possible to eliminate Cyber Risk, only reduce it
- 1st Party Risk
- 3rd Party Risk
- Scenario – Internal IT
- Scenario – Independent IT Guy
- Scenario – Outsourced IT/Managed IT Provider

Shared Risk Model

- Each vendor may/may not accept certain risks
- Avoid single supply chain areas
- Cash flow management
- High cost of sales markets



Shared Risk Responsibility Model

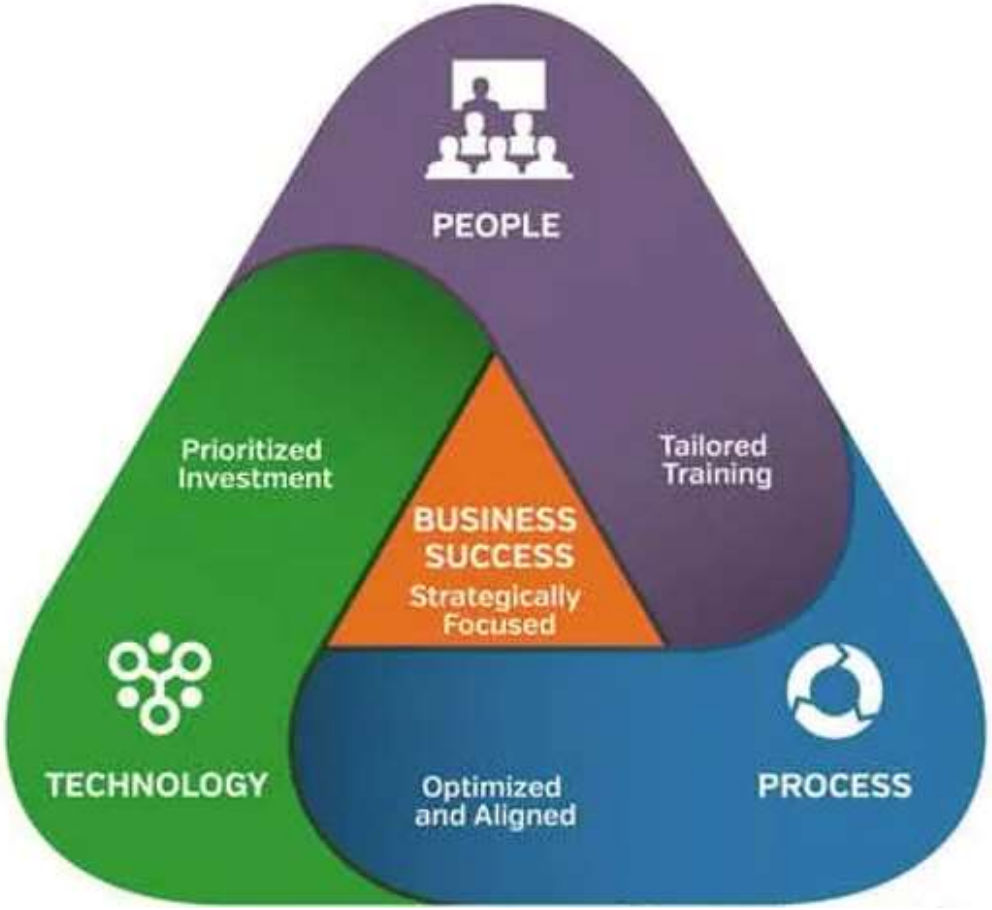
	Primary Responsibility	Supporting Technology	Security	Regulatory
Microsoft Responsibility	**Microsoft Infrastructure** Cloud Uptime Backend Hardware Maintenance	**Microsoft 365 Data Replication** DC to DC Geo-redundancy **Recycle Bin** Limited, short-term data loss recovery (no point in time recovery)	**Infrastructure Level** Physical Security Logical Security App-level Security User/Admin Controls	**Role as Data Processor** Data Privacy Regulatory Controls Industry certifications HIPAA, Sarbanes-Oxley
↑ Third-party Risk				
Internal IT / MSP Responsibility	**Infrastructure** Network / Security tools Asset Inclusion Maintenance	**Tools** Windows Patching Backup EDR anti-malware Email filtering *	**Systems Level** Basic Security Tools Configuration Optional additional security tools *	**Role as Custodian** Implement data owner policies Make general security recommendations
First-party Risk ↓				
Client Ownership / End-user Responsibility	**Your Data** Network data or in Microsoft 365 On-site, via email or remote	**Usage** Internal Security Officer Your policies / decisions Framework based security Lifecycle management	**Data Level** Security awareness training End-user actions PC/Cloud backups Shadow IT	**Role as Data Owner** Know your applications Classify data Comply with regulations Supply Chain Risk
Risk Transfer ↓				
Cyber-insurance Carrier Responsibility	**Your Policy** Appropriate Coverage Appropriate Amounts Exclusions	**Usage** Application quality Risk assessments Incident response	**Data Level**	**Role as Insurer** Compliances Pay for known risk Avoid paying unknown risk

* Actual tools may vary

CIS Control 15.3
Classify Service Providers

Cybersecurity At a Glance

- There is no “magic bullet” of cybersecurity
- Every security tool will eventually fail
- There is no such thing as being 100% secure
- Google & Microsoft spend billions on cybersecurity, yet they are regularly breached
- Most breaches are from human error
- CIS Critical Security Controls (CIS Controls) are a prioritized set of Safeguards



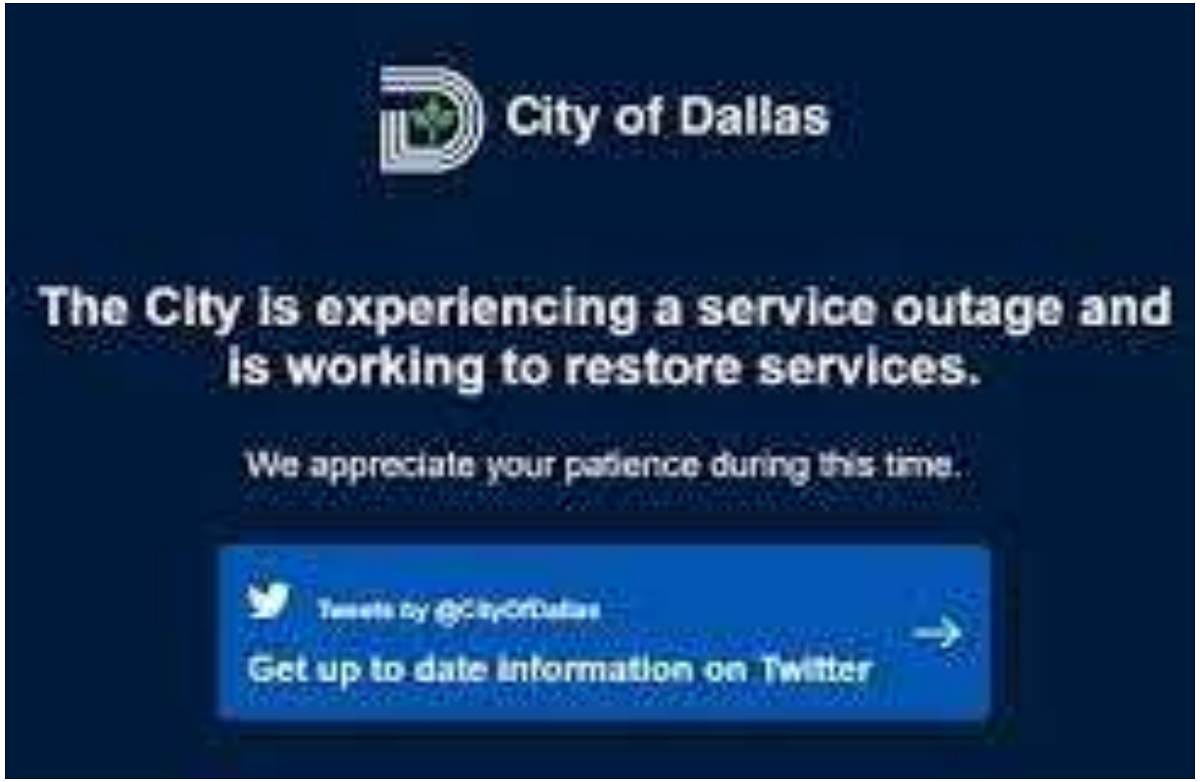
68% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering- **Verizon 2024 DBIR report**

CIS Implementation Group 1

What’s Changed in the Last 3 Years

City of Dallas Breach

- Access gained through stolen credentials
- Cybercriminals were inside the City of Dallas network for several weeks before being discovered
- Financial losses of at least $8.5M, plus 26,000 residents’ data was disclosed



City of Dallas

The City is experiencing a service outage and is working to restore services.

We appreciate your patience during this time.

Tweets by @CityOfDallas

Get up to date information on Twitter

What’s Changed in the Last 3 Years

Caesar’s & MGM

- Access gained through social engineering that led to MFA bypass
- Caesar’s paid a $15M ransom
- Both organizations had MFA

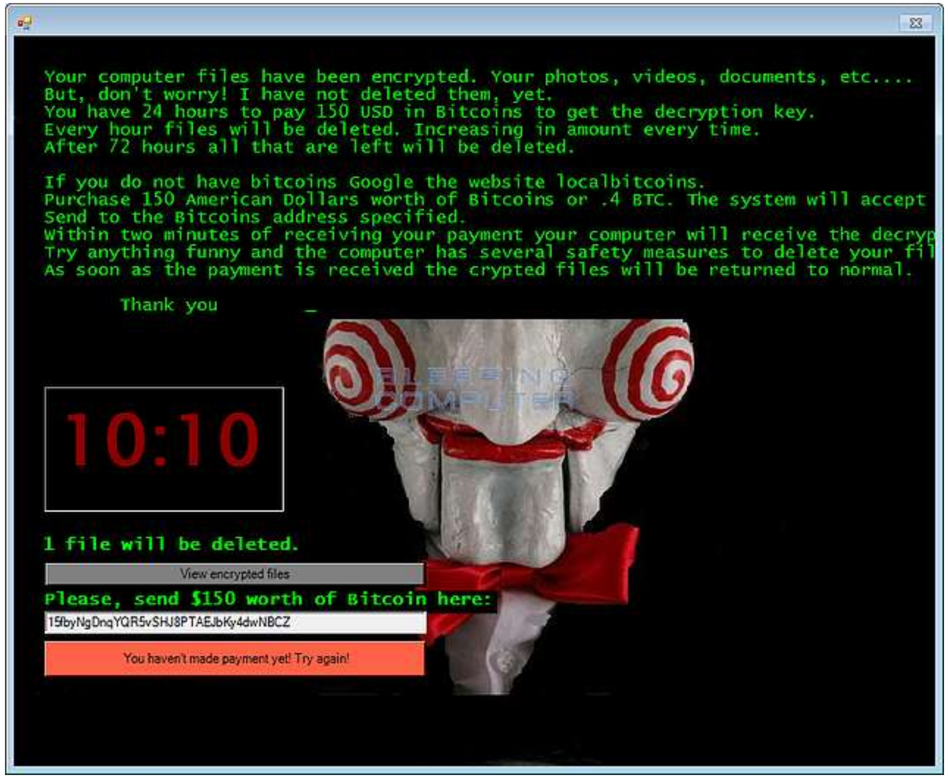
What’s Changed in the Last 3 Years

Dollys.com

- Russian hackers gained access, exfiltrated their data, then locked their data with encryption
- Dollys.com paid the ransom in exchange for deleting exfiltrated data that included account logins, credit card info, customer info
- The hackers kept the ransom payment but published the data to the Dark Web anyway

Exponential Increase in Cyber Risk

- Cybercriminals are…
  - More sophisticated
  - Have AI tools available
  - More patient
  - Willing to go to multiple levels of extortion to get paid
- Anatomy of a Cyber Attack
  - Hacker gains a persistent foothold into your network using phishing and/or Dark Web credentials
  - Now that they have access, they can patiently exfiltrate and sift through your data, looking for your cyber insurance coverage, intellectual property, client information, vendor information, etc.
  - After disabling your antivirus software and deleting your backups, that's when they encrypt your data and make the initial ransom demand
  - Then they hit you with multiple levels of extortion to make sure you pay



```
Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryp
Try anything funny and the computer has several safety measures to delete your fil
As soon as the payment is received the crypted files will be returned to normal.

        Thank you     _

10:10

1 file will be deleted.
Please, send $150 worth of Bitcoin here:
15fbyNgDnqYQR5vSHJ8PTAEJbKy4dwNBCZ
You haven't made payment yet! Try again!
```

What’s Changed in the Last 3 Years

Remote Work Trends

- Pandemic increased Remote Work options
- Decentralized Workforces
- Hybrid work models are common
- More cloud applications
- Focus on Employee Mental Health
- Cybersecurity is more challenging in a Remote Work scenario
- The War for Talent

What it Means to be a Cyber Focused CEO

Make Cybersecurity a Priority

- Educate yourself, subscribe to Cybersecurity Threat feeds
- Follow company Cybersecurity processes & procedures
  - Complete Annual Cybersecurity training
  - Follow processes for financial transactions
- Engage with your IT team about Cybersecurity
  - Trust but verify
  - Give them a seat at the Executive table
- Maintain Cyber Insurance
  - Conduct a Risk Assessment

Yesterday’s Cybersecurity isn’t Enough

- The business world has changed
  - No longer operating in the walled fortress of your office
  - Remote users, apps/data in the cloud
  - Antivirus & Firewall at the office isn’t enough

What it Means to be a Cyber Focused CEO

The NEW Basic Cybersecurity

- End Point Detection & Response (EDR) instead of Antivirus
- Multi-Factor Authentication & Single Sign On
- Security Awareness Training, Phishing Simulations, & Dark Web Monitoring
- Cybersecurity Monitoring – SIEM/SOC as a Service, Managed Detection & Response, don’t forget to monitor cloud apps/data, if budget allows
- 3rd Party IT Audits
  - Vulnerability Assessments
  - Penetration Tests

What it Means to be a Cyber Focused CEO

What's Next in Cybersecurity

- Zero Trust Architecture
- Cybersecurity Monitoring – SIEM/SOC as a Service, Managed Detection & Response, don't forget to monitor cloud apps/data
- Don't forget backups (both local and cloud), Incident Response, Risk Assessments, and other Cyber Assessments

Summary – 5 Things to Do NOW

Cybersecurity for CEOs Phase 2 - Summary

- A lot has changed – Remote Work, Cloud, Cyber Threats, Cyber Risk, Cyber Insurance
- Step 1 – Educate yourself on Cyber Threats
- Step 2 – Follow Cybersecurity processes
- Step 3 – Engage your IT team about Cybersecurity
- Step 4 – Maintain appropriate Cyber Insurance
- Step 5 – Implement the NEW Basic Cybersecurity
- Bonus Step 6 – Start researching what's NEXT in Cybersecurity

THE FULCRUM GROUP

Agenda

- Any questions?

The Fulcrum Group, Inc.
1670 Keller Parkway, Suite 130
Keller, TX 76248

Phone: 817-337-0300
Help Desk: 817-898-1277
Web: www.fulcrum.pro
Support: helpdesk@fulcrumgroup.net