UNIVERSITY OF TEXAS ARLINGTON

XYZA SOLUTIONS CORP.

INTRODUCTION AND CYBERSECURITY POSTURE

XYZA Solutions Corp. Leadership
Chris, CEO
David, CFO
Don, CIO
David, VP Manufacturing
Sandra, General Counsel
Alex, VP HR
Declan, Engineering Director

Cybersecurity Division
Maria Tapia, Team Lead
Rose Ramirez
Diego Martinez
Michael Aiyedun
Jeremiah Pitts

AGENDA ITEMS:

- Technical Overview and Background
- Current Standing
  - Infrastructure Environment
  - Security Posture and Culture
- Recommendations
  - Industrial Control System (ICS) Security
  - Cloud
  - Cybersecurity Awareness Program
  - Disaster Recovery and Business Continuity
- Next Steps

TECHNICAL OVERVIEW AND BACKGROUND

TECHNICAL OVERVIEW AND BACKGROUND (1/3)

Data Breach – Release of secure information into an insecure environment. A data breach may be intentional or unintentional.

Malware – (Short for **Mal**icious Soft**ware**) Software designed to disrupt, damage, or intrude into a computer.

Ransomware – Malware that compromises or disables a user's system until the user pays a ransom.

Classically ransomware involves encrypting the victim's data, rendering it unusable to the victim who owns it until the victim pays the extortionists for a decryption key.

Source: The CyberWire Glossary - https://thecyberwire.com/glossary

TECHNICAL OVERVIEW AND BACKGROUND (2/3)

Cloud Computing[1] – Internet-based computer storage and operations, conducted on the Internet as opposed to local devices.

Industrial Control System (ICS)[1] – A system that controls industrial processes.

Motion control systems for industrial robots and process control systems that regulate variables like pressure, flow, or temperature are examples of industrial control systems.

Cybersecurity Hygiene[2] – Cyber hygiene is a set of habitual practices for ensuring the safe handling of critical data and for securing networks.

It's like personal hygiene, where you develop a routine of small, distinct activities to prevent or mitigate health problems.

Source 1: The CyberWire Glossary - https://thecyberwire.com/glossary

Source 2: Tanium - https://www.tanium.com/blog/what-is-cyber-hygiene-and-why-does-it-matter/

TECHNICAL OVERVIEW AND BACKGROUND (3/3)

Technical Debt – Similar to financial debt:

The ***principal*** is all the work that must be done *to modernize the entire technology stack*.

This includes deferred maintenance or upgrades below the app layer, modifications to comply with data standards, etc.

The ***interest*** is the *complexity tax that every project pays today*.

It derives from the need to work through fragile point-to-point or batch data integrations, harmonize nonstandard data, and create workarounds to confront risk and meet business needs.

Source: MicKinsey & Company - https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-debt-reclaiming-tech-equity

Source: Equifax breach settlement email: What to know about the upcomingpayme(fastcompany.com)

EXAMPLES (1/2)

Equifax had a security incident that exposed personal information from 143-148 million Americans in 2017.

EXAMPLES (2/2)

ISOFH, healthcare technology company, leaked 12 million records on patients including highly sensitive diagnoses

Source: Vietnamese Tech Firm iSofH Leaked 12 Million Sensitive Patient Records | Cyware Alerts - Hacker News

CURRENT STANDING

AREAS OF CONCERN

Mission Critical Industrial Control Systems are Insufficiently Protected

Significant Technical Debt

Will hinder long-term, strategic initiatives and redirect resources to lower value, redundant, or deprecating systems

High Likelihood of Material Impact Due to a Cybersecurity Event

Cybersecurity practices misaligned with company priorities

RECOMMENDATIONS

RECOMMENDATIONS

- Increasing ICS Security Based on Industry Standards
- Addressing Infrastructure Constraints and Tech Debt
  - Initiate Cloud and Tech Debt Initiatives
    - What should be migrate and when?
- Combating Ransomware via:
  - Cybersecurity Awareness Program
  - Disaster Recovery and Resiliency Program

INDUSTRIAL CONTROL SYSTEMS

ICS control the physical world and IT systems manage data

- Demilitarized Zone (DMZ) network architecture with firewalls
- Having separate authentication mechanisms and credentials for users of corporate and ICS networks
- Internet access (i.e., server, email, remote access, etc.) is typically permitted on the corporate network but should **NOT** be allowed on the ICS network.

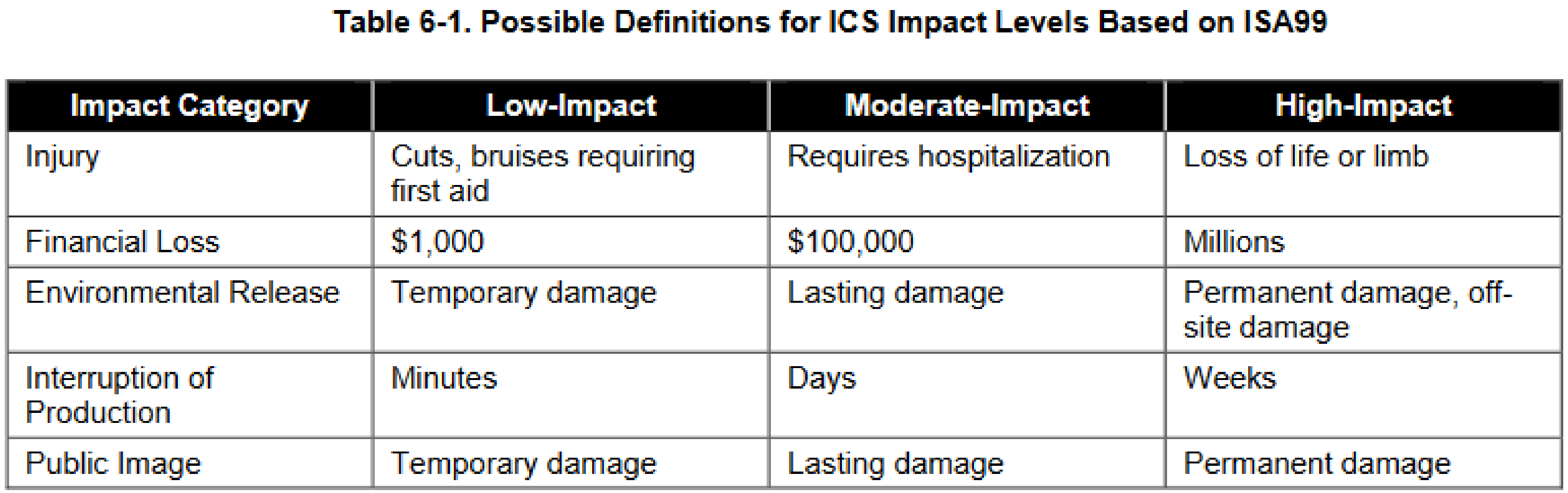


Table 6-1. Possible Definitions for ICS Impact Levels Based on ISA99

Impact Category	Low-Impact	Moderate-Impact	High-Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss	$1,000	$100,000	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Minutes	Days	Weeks
Public Image	Temporary damage	Lasting damage	Permanent damage

Source: NIST Special Publication 800-53

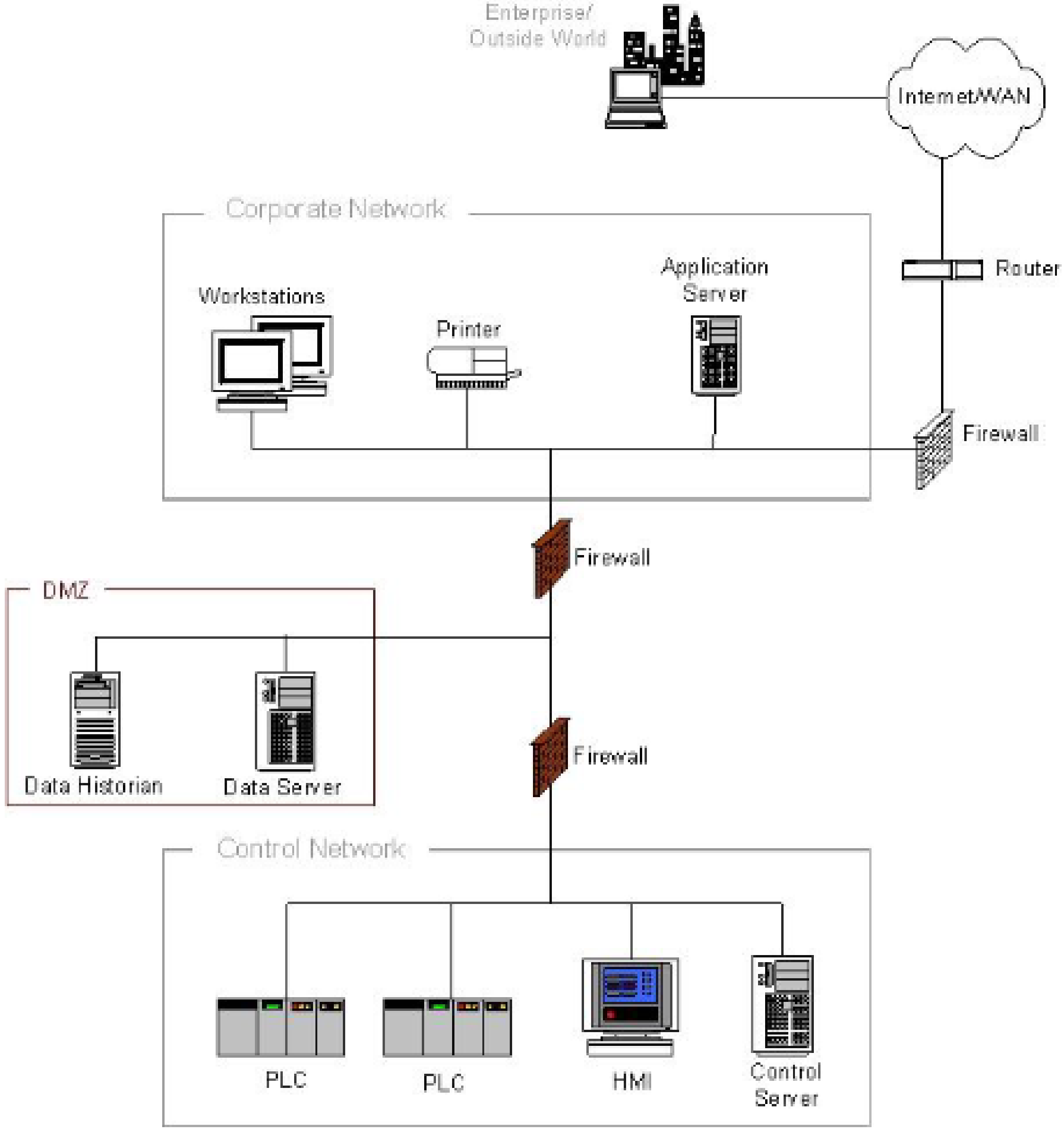
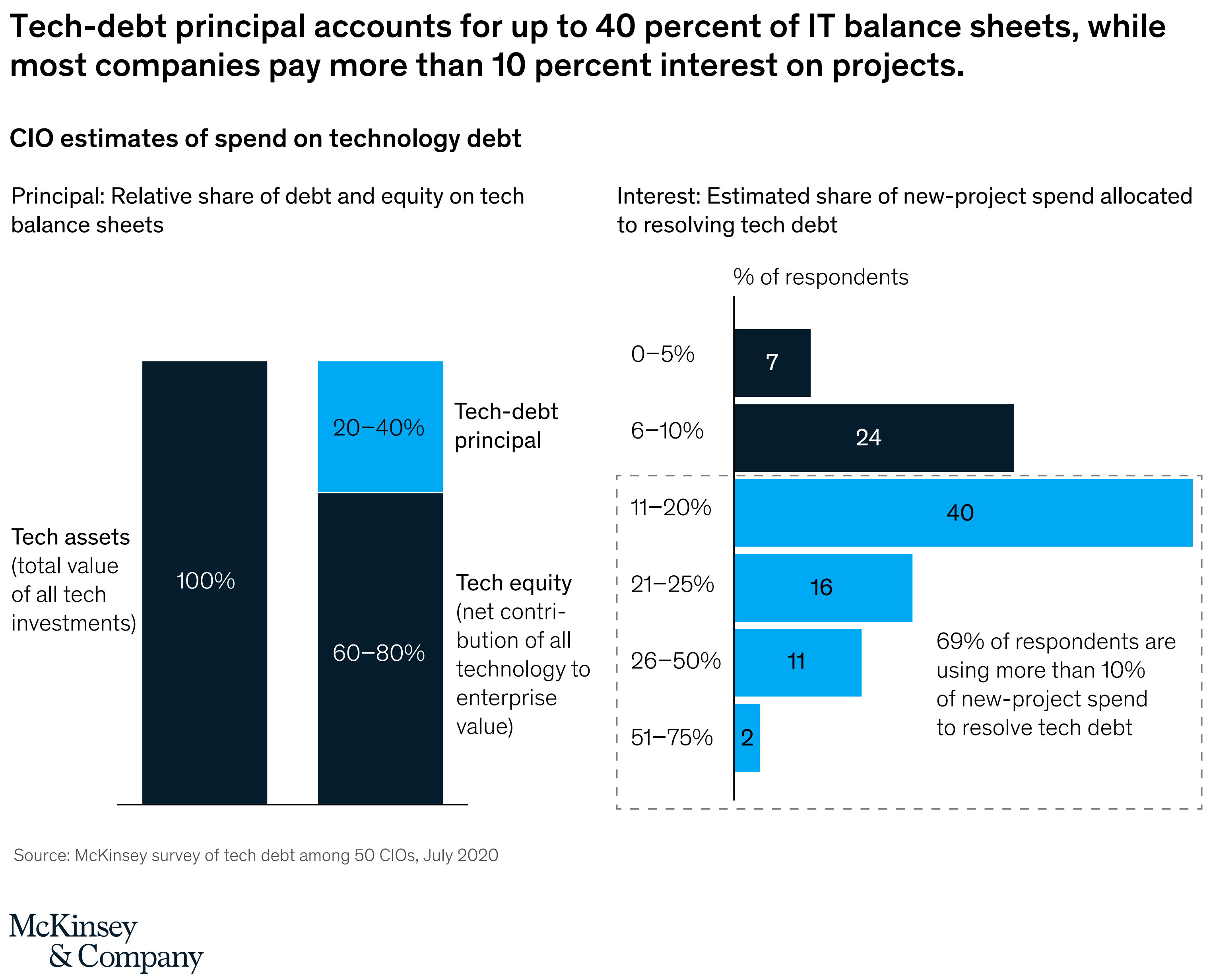


Figure 5-4. Paired Firewalls between Corporate Network and Control Network

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

TECH DEBT - FINANCIAL AND STRATEGIC SETBACKS



Tech-debt principal accounts for up to 40 percent of IT balance sheets, while most companies pay more than 10 percent interest on projects.

CIO estimates of spend on technology debt

Source: McKinsey survey of tech debt among 50 CIOs, July 2020

McKinsey & Company

Source: MicKinsey & Company - https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-debt-reclaiming-tech-equity

TECH DEBT – CLOUD BENEFITS AND LIMITATIONS

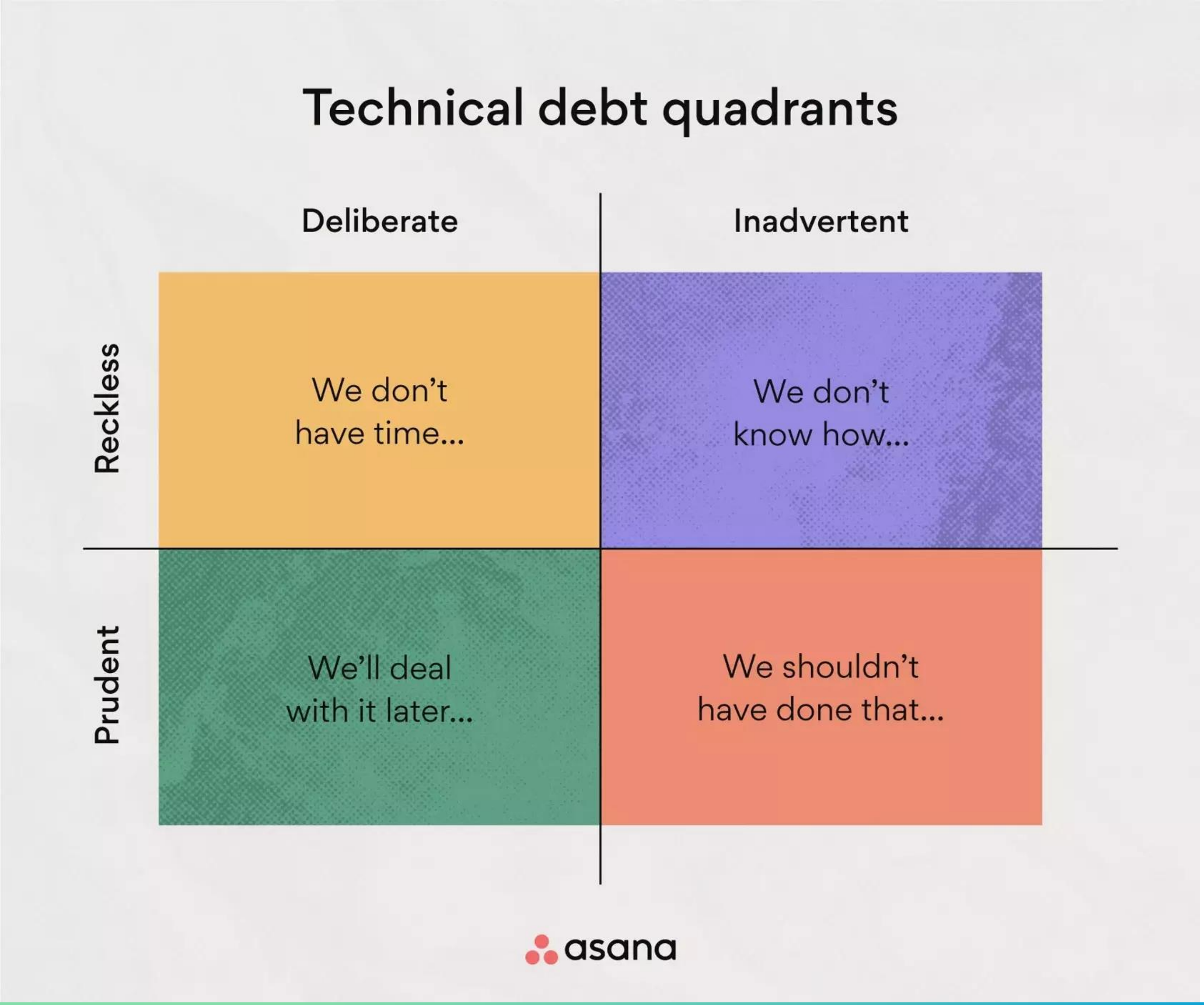
Benefits:

- Faster time to market
- Scalability and flexibility
- Cost savings
- Better collaboration
- Advanced security
- Data loss prevention

Limitations:

- Risk of vendor lock-in
- Less control over underlying cloud infrastructure
- Concerns about security risks like data privacy and online threats
- Integration complexity with existing systems
- Unforeseen costs and unexpected expenses

Source: Google Cloud - https://cloud.google.com/learn/advantages-of-cloud-computing



Technical debt quadrants

	Deliberate	Inadvertent
Reckless	We don’t have time...	We don’t know how...
Prudent	We’ll deal with it later...	We shouldn’t have done that...

TECH DEBT - PLANNING

- Determine what applications and systems should go to the cloud, be consolidated, or retired.
  - Initial planned phase development
- Estimate costs of different plans and options, balancing risk, budget, and people resources.
- Determine areas for training and development as well as temporary outside resources.

Image Source: https://asana.com/resources/technical-debt

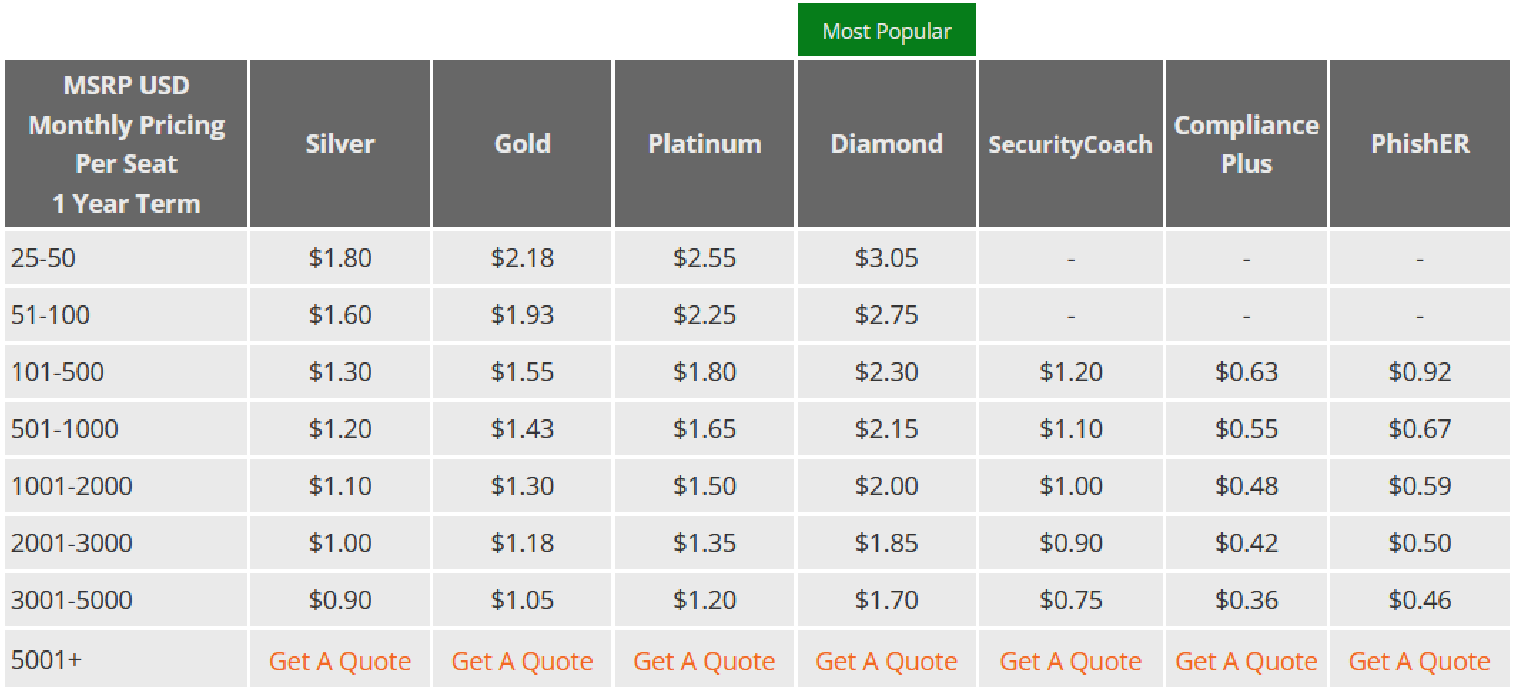
RANSOMWARE - CYBERSECURITY AWARENESS PROGRAM

Cybersecurity Awareness Program:

- Mitigate malicious software downloads
- Learning modules and success recognition
- A mixture of in-house and cybersecurity awareness company education (i.e. KnowBe4).

KnowBe4 Example:

- Estimating 2000 users at a monthly pricing for a 1-Year Term Diamond Contract is **$48,000**
- Estimating 4000 users at a monthly pricing for a 1-Year Term Diamond Contract is **$81,600**



				Most Popular			
MSRP USD Monthly Pricing Per Seat 1 Year Term	Silver	Gold	Platinum	Diamond	SecurityCoach	Compliance Plus	PhishER
25-50	$1.80	$2.18	$2.55	$3.05	-	-	-
51-100	$1.60	$1.93	$2.25	$2.75	-	-	-
101-500	$1.30	$1.55	$1.80	$2.30	$1.20	$0.63	$0.92
501-1000	$1.20	$1.43	$1.65	$2.15	$1.10	$0.55	$0.67
1001-2000	$1.10	$1.30	$1.50	$2.00	$1.00	$0.48	$0.59
2001-3000	$1.00	$1.18	$1.35	$1.85	$0.90	$0.42	$0.50
3001-5000	$0.90	$1.05	$1.20	$1.70	$0.75	$0.36	$0.46
5001+	Get A Quote	Get A Quote	Get A Quote	Get A Quote	Get A Quote	Get A Quote	Get A Quote

RANSOMWARE - DISASTER RECOVERY & BUSINESS CONTINUITY

Disaster Recovery and Business Continuity

- Develop plans for different, likely scenarios
- Periodically practice via table-top exercises (a type of role play and scenario-based training) and close replications or simulations of the scenarios
- Periodically update plans based on company needs and cybersecurity risk

NEXT STEPS

OUR ROLE AND GOALS

- Reducing the likelihood of material impact to the organization due to a cybersecurity event.
- Increasing the likelihood of successful cybersecurity event response and remediations per business objectives.
- Empowering the board and executive leadership team to make more informed business and daily living decisions.

NEXT STEPS AND REQUESTS

Board

- Funding discussions for each program
- Regularly discussing and addressing cybersecurity topics at each board meeting
- Include Steve in board meetings and communications regarding changes in IT and company strategy

Executive Leadership

- Discuss with Steve regarding any questions, concerns, or recommendations regarding cybersecurity practices

THANK YOU