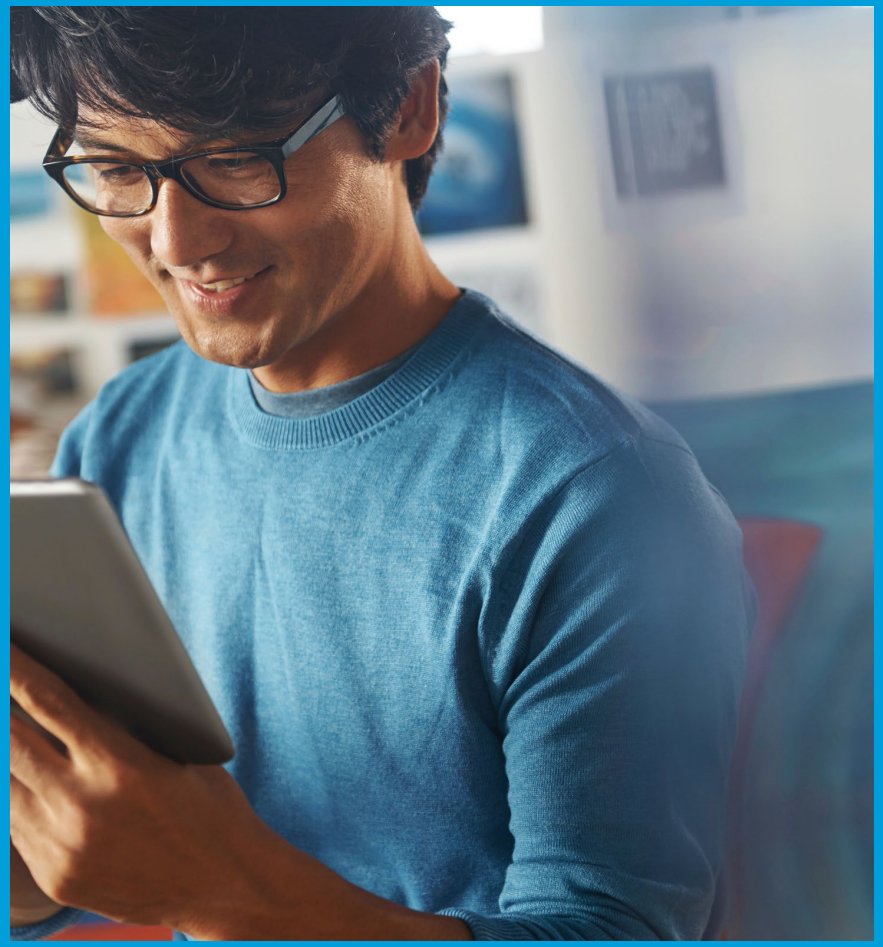
2023 Information Security Forum

Risk-Based Cyber



Bill Higginbotham
Associate Director
AT&T Cybersecurity Consulting

29 March, 2023

AT&T Business

Agenda

- Opening Remarks
- Quick Risk Management Overview
- Identifying Critical Systems
- Measuring Cybersecurity
- The Risk of Cyber
- Additional Risks Cyber has Introduced
- Wrap-up

Introduction

AT&T Business

AT&T Cybersecurity:

- William Higginbotham, Associate Director, Cybersecurity Consulting

ISF Attendees:

- Cybersecurity
  - CIO
  - CISO
  - Directors
  - Engineers
  - Analyst
- Business
  - Operations
  - Finance
  - HR

Quick Risk Management Overview

Risk Categorization

- Simple – Internal/External/Strategic
- Complex – Operational/Business/Supplier/Financial/Reputational/Technology/Schedule/ Programmatic/Information Security/Resources/Infrastructure/Industrial Control Systems/Quality/Process/Project/HR/Payroll/Safety/ etc …etc …etc …

Most common approach to cybersecurity is the umbrella approach to secure "Everything"

Risk based cybersecurity focuses on high security maturity for critical systems first.

Quick Risk Management Overview

Actions to Address Risk

- Accept – May cost more to fix than the damage it would cause
- Eliminate – Stop doing the function
- Mitigate – Buy down risk (in this case with cyber security)
- Transfer – Insurance, Partnerships, Contracts

Risk Based Cyber Approach:
The Singular Purpose of Cybersecurity is to Mitigate (Reduce) the Risk Presented by Using IT.

Identifying Your Critical Systems

The leader must decide what systems and applications are vital to the operation of the business

- Informed by the business units
- Completed Business impact Analysis (BIA)
- Functional Mission Analysis (FMA -C)
  - List u nacceptable outcomes

Risk Based Cyber Approach:
Prioritize in order of unacceptable outcomes, business impact, and then advice of the business unit.

Identifying Your Critical Systems

Additional considerations for prioritization of critical systems

- Deprecation exercise
  - If you have 5 critical systems and power availability went down to 80%, which system would you turn off first?
  - Which system would you turn off last?
- Actually “Exercise” your deprecation list (during off -hours or slow times)
- Can you still perform your mission at 80% / 40% / 20%?

Risk Based Cyber Approach:
The order in which you deprecate is the reverse of prioritized systems

Identifying Your Critical Systems

You have identified the priority order of critical systems using cyber:

- Safety/Industrial Control System
- Operations
- Financial
- Information Systems
- Payroll

The IT, applications, and cyber capabilities of these systems are th e focus of your cybersecurity efforts

Now measure the cybersecurity maturity of each of these systems

Maturity Level	Keywords	Description
0	None, Nonexistent	There is no evidence of the organization meeting the objective.
1	Ad-hoc, Initial	The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.
2	Consistent, Repeatable	The organization has a consistent overall approach to the meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
3	Compliant, Defined	The organization has a documented, detailed approach to meeting the objective, and regularly measure its compliance.
4	Risk-based, Managed	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
5	Efficient, Optimized	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.

AT&T Business

Measuring Cybersecurity Maturity

Based on what???

- Safety/Industrial Control System – NIST 800-53 CSF + NERC
- Operations – Texas Cybersecurity Framework (TCF)
- Financial – NIST 800-53 CSF + PCI/DSS
- Information Systems - TCF
- Payroll – NIST 800-53 Custom Controls Catalog

Risk Based Cyber Approach:
Pick the appropriate control sets to address individual "Systems"

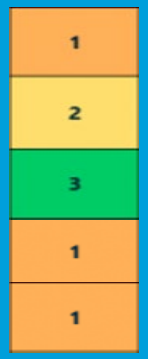
Measuring Cybersecurity Maturity

Maturity Level	Keywords
0	None, Nonexistent
1	Ad-hoc, Initial
2	Consistent, Repeatable
3	Compliant, Defined
4	Risk-based, Managed
5	Efficient, Optimized

State of Texas Maturity Targets:

- TCF – 3.0 or higher
- Risk-based cyber – 4.0 or higher

- Safety/Industrial Control System
- Operations
- Financial
- Information Systems
- Payroll



Who gets the money???

Risk Based Cyber Approach:
All systems on list below target score (These are Critical Systems)

What about all the other systems???

Less than critical systems still need attention

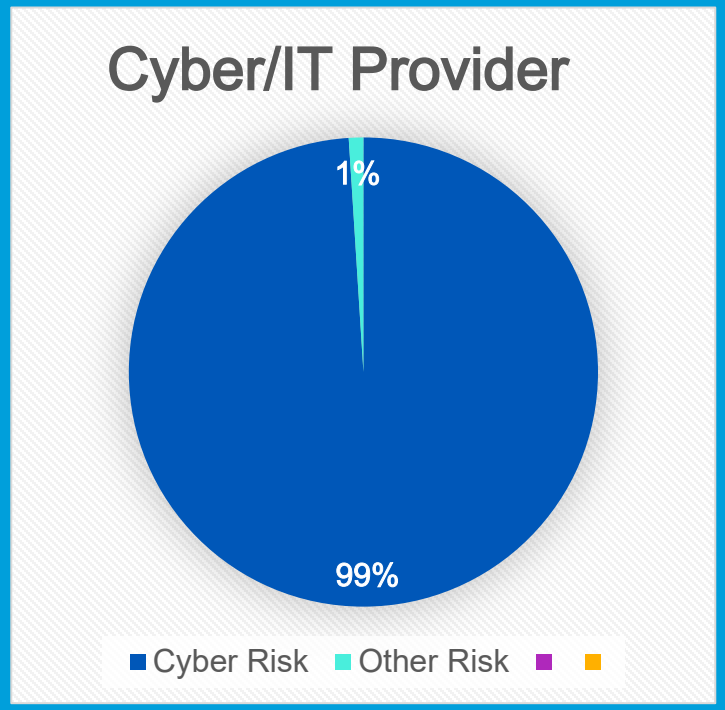
- Perform same exercise as critical systems
- Further categorize systems into lower risk categories
- Use same control framework for remaining systems (Enterprise -wide)
- Consider risk transfer
- Consider risk elimination

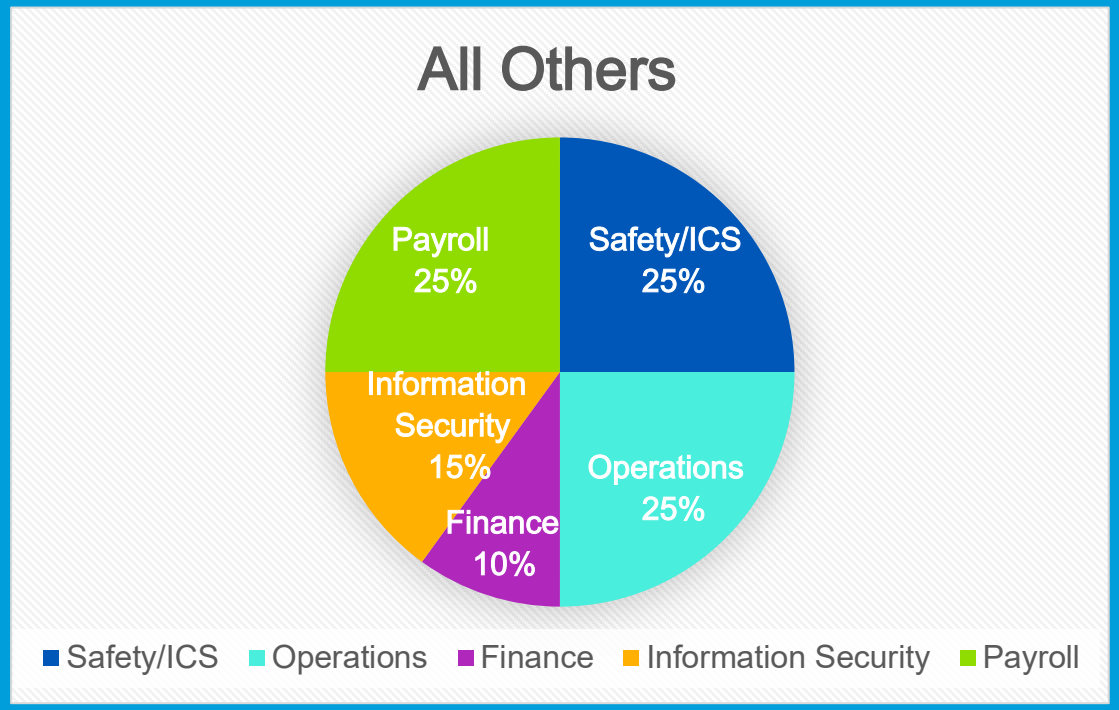
Risk Based Cyber Approach:
Recommend 3 levels of risk categorization. Third level risks should be considered for transfer or elimination.

The Risk of Cyber

Concept of Cyber Risk

- If primary function is cyber/IT, then cyber risk is everything
- If primary function is other, then cyber risk is a multiplier to determine organizational risk





1st Additional Risks Cyber has Introduced

Insurability

- Low cybersecurity maturity affects cyber insurance
  - Higher premiums
  - Lower payouts
  - Insurance caps
  - Uninsurability

Cybersecurity is risk mitigation. Lower maturity here will increase the cost of other options

Risk Based Cyber Approach:
Risk transfer in the form of cyber insurance is off the table for high risk organizations -

2nd Additional Risks Cyber has Introduced

Overall Cost of Government

- Low cybersecurity maturity affects business/government credit ratings
  - Bond financing
  - Loan financing
  - Higher interest rates/payments
  - Less discretionary funding

This trend is currently building momentum and will continue to get worse. Low maturity means higher risk to financiers.

Risk Based Cyber Approach:
Spend money on cybersecurity or spend it on interest payments

Wrap Up!