Ray A. Rothrock
Chairman & CEO, RedSeal, Inc.
Venrock, Partner Emeritus
Forbes Midas List
Former Chair National Venture Capital Association
Member of the MIT Corporation
Vice Chairman, UTIMCO
Distinguished Alumnus Texas A&M
Director – Check Point Software Technology, Ltd.
Trustee Carnegie Institute of Science
Director – Roku, Inc.
Up and to the Right - Bassist
April 2019
HOW MANY OF YOU THINK WE ARE WINNING THE CYBER WAR?
TRENDS SUGGESTS THE HACKERS ARE WINNING

- **Disruption**: Worms & Viruses
- **Crime**: Spyware & Bots
- **Organized**: APTs, Zero Day Threats

**Number of Attacks**
- **1980**
- **1990**
- **2000**
- **2010**
- **2020**

**Network & Host Security**

**NGFW & Sandboxing**
2013 TIPPING POINT ⇒ 2018

TARGET

RUSSIA (CHINA)
THE HACKER IS ALREADY INSIDE.
AND AT WHAT COST?

$2 Trillion
By 2019
$1 Trillion
Intellectual Property
Forbes, 2016

TRUST
CONFIDENCE
Organizations still fail basic cyber hygiene tests.

Organizations are rarely in compliance all of the time, if ever.

Organizations struggle to stay prepared to respond to latest threats.

Time is our enemy. Organizations can’t respond fast enough.

Organizational leaders face tough questions, changing risks, and unknown threats.

Their customers wonder.
RESILIENCE DIVIDEND: BEING STRONG IN A WORLD WHERE THINGS GO WRONG*

Dr. Judith Rodin
President, Rockefeller Foundation

Book originally published 2014
A MODEL FOR RESILIENCE

THE HUMAN BODY
A NEW STRATEGY IS REQUIRED

MY PATTERN RECOGNITION SUGGESTED NEW THINKING WAS NEEDED:

RESILIENCE
RESILIENCE IS A STRATEGY

Process

Technology

People

ACROSS THE ENTERPRISE
TECHNOLOGY

MOST SYSTEMS WERE NOT BUILT WITH RESILIENCE IN MIND
THE PATH TO DIGITAL RESILIENCE

1. UNDERSTANDING and VISIBILITY
2. MEASUREMENT
3. COMPLIANCE
4. ACCELERATE RESPONSE
THE BUILDING BLOCKS OF DIGITAL RESILIENCE

UNDERSTAND

your network with as-built model

MEASURE

benchmark and set targets

MANAGE

standard policies and VERIFY compliance

ACCELERATE RESPONSE to vulnerabilities, incidents, and network interruptions
UNDERSTAND THE DIGITAL INFRASTRUCTURE:
NETWORK AND DATA

DATA MOVES ON A PATHWAY.

DATA PATHWAYS ARE PROGRAMMED.

YOU DO NOT KNOW EVERY PATH IN A MODERN ENTERPRISE

76% Of CEOs believe they have an accurate blueprint of their network infrastructure

100% Of RedSeal customers find network devices, subnets, and pathways that weren’t on the blueprint, if they had one
YOU CAN MEASURE RESILIENCE

PREScribe Actions to IMPROVE RESILIENCE.

- Vulnerabilities in Network Context
- Routing Configurations - Secure and Proper
- Pathways - Known, Unknown or Inappropriate Pathways
WE ARE A LONG WAY FROM RESPONSIVE

40% rank detection as their strongest cyber capability

PERCEPTION
It takes an average of
6 HOURS to detect an incident

REALITY
Studies reveal very different answers
24 HOURS
49 DAYS
99 DAYS

Source: RedSeal Resilience Report
ACCELERATE RESPONSE | TECHNOLOGY

MUCH TO DO WHEN UNDER ATTACK.
TIME IS NOT YOUR FRIEND.

INCIDENT LOCATION
BLAST RADIUS
ALL POSSIBLE PATHS
WHAT DATA AND ASSETS ARE AT RISK
WHAT ARE MY OPTIONS
INITIATE CONTAINMENT
VALIDATE CONTAINMENT
ASSESS DAMAGE
REPAIR & RECOVER
NO STRAIGHT LINE TO SUCCESS

SKILLED PEOPLE, DEFINED AND REHEARSED PROCESSES, AND TECHNOLOGY ARE INVOLVED
RESILIENCE IS A STRATEGY

Starts in the C-Suite then THROUGHOUT THE ENTERPRISE
WE CAN DO THIS: DIGITAL RESILIENCE

We **must** be better prepared, through digital resilience.

We **must** create trust, confidence, and capability.

Starts in the C-suite
KEY TAKEAWAYS from D.R.

• Frame RESILIENCE as a business issue, not a cyber security issue.

• Ask “What can go wrong?”

• Basic cyber training for everyone.

• Share the truth about visibility, infrastructure and issues.

• Put experts at the table.

• Establish metrics and measure often.

• Preparation is critical to your cyber strategy.
WHAT'S A BOARD TO DO

• Frame RESILIENCE & CYBER as business issues, not a technical cyber security issue.

• Basic cyber training for everyone. Step and repeat.

• Create a standing Cyber Resilience Committee.

• Ask “What can go wrong?”

• Share the truth about visibility, infrastructure and issues.

• Put experts at the table.

• Establish metrics and measure often.

• Resilience requires preparation. Both are critical to your cyber strategy.
WHAT’S A PERSON TO DO

• Learn to recognizing a phishing email – delete it.
• Use two-factor authentication wherever you can.
• Make backups of your computers (ransomeware).
• Patch and upgrade your hardware and software.
• Manage your passwords. Change your passwords.
• Don’t do sensitive business on public WiFi.
• Check regularly and lock your credit bureau records.
• Think before you act on email, browsers and your phone.
MY VISION

A world where DIGITAL RESILIENCE delivers CONFIDENCE in the face of cyber attack.
QUESTIONS