Keeping Your Eyes on the Goal
What Boards Need to Know About Cybersecurity Risk
The content of this presentation does not reflect the view of my current company, Techtronic Industries Company Limited. The presentation you are about to enjoy is comprise of my personal journey, a compilation of a lot of reading, research, experiences, and what has worked for me.
No one cares what you can do. Everyone cares what you can do for them.
48% Top 5 responsibility
Organization wide Cybersecurity Culture

46% Rates their Cyber Risk Management strong

55% CISO provides periodic updates to the Board

84% Ability to Educate and Collaborate across the business
WHAT IS OUR JOB?

PROTECT

PROFITS
"Where there is no vision, there is no hope." — George Washington Carver
C + I = A

VISION

EXECUTION

Patience.
- Bad cybersecurity metrics
- Every program is different

"Don’t tell people your plans. Show them your results." — Unknown
To add value, subtract complexity.
REMEMBER, OUR JOB IS TO PROTECT PROFITS
"If you want to go fast, go alone. If you want to go far, go together." — African Proverb
The Three Unanswered Board Questions That Drive Cybersecurity Investment*

1. How much should I spend on Cybersecurity?
2. How does our program compare to others?
3. What metrics should CISOs report to the board?

*According to Gartner
Where you stand is what you see.
“The main goal of our program is to reduce systemic risk across all business units, which allows us to enable growth and remain competitive”

“If you can’t describe what you are doing as a process, you don’t know what you’re doing.” — W. Edwards Deming
<table>
<thead>
<tr>
<th>PTS</th>
<th>W</th>
<th>L</th>
<th>+/-</th>
<th>SA</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAV%</td>
<td>SHG</td>
<td>SOG</td>
<td>SH%</td>
<td></td>
</tr>
<tr>
<td>PIM</td>
<td>SVS</td>
<td>GWG</td>
<td>SOA</td>
<td>MIN</td>
</tr>
<tr>
<td>PPG</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
"A dead thing can go with the stream, but only a living thing can go against it." — G. K. Chesterton
Maturity by Security Capability

- Identify
- Protect: 4
- Detect: 2.5
- Respond: 3.5
- Recover: 2
- OT Security: 1

Maturity
# Simplified Business Impact Analysis

## Critical Assets (Business Processes)
- What are the business units that make the most profit?
- What are the biz processes that make the most profit?
- What are the business-critical applications?
  - Payroll
  - ERP
  - IP

## Threats (Highest Likelihood)
- What are the biggest threats to the assets?
- Threats to CIA
- Which one will be most impactful...
  - If data is disclosed?
  - If data is altered?
  - If access is denied?

## Vulnerabilities (Impact)
- What vulnerabilities are present on the servers that will allow these threats to have a critical impact to the organization?
- Get a listing of the following:
  - Servers that contain the critical assets
    - What is the exposure point?
    - What are the vulnerabilities?
  - Find alignment and specific data
- THIS COLUMN BECOMES OUR SECURITY ROADMAP & STRATEGY
- Do it quarterly
Let’s Make Cybersecurity a Choice

Balance the **Need to Protect** against the **Need to Run** your Business

*According to Gartner*
LET THE BUSINESS DECIDE

High Business Value

Bad Risk Posture (High Risk)

Low Business Value

Good Risk Posture (Low Risk)

Legal

Product Engineering

Intellectual Property

OT
Board is not pleased

BU looks terrible
Executive not engaged

Report to Board

Prioritize remediation investments
Measure & Report Variation
Negotiate PLA w/ BU
The NIST CSF

The Business

The Board

DiRECTOR™ ontology. © DDN LLC
Get more done by doing less.
YOU ARE WHAT YOU DO.

NOT WHAT YOU SAY YOU'LL DO.

"You are what you do, not what you say you'll do." — Carl Jung
Credits

Research:

- Book: The Great Reboot by Bob Zukis, Paul Ferrillo, Chris Veltsos
- Digital Directors Network: https://www.digitaldirectors.network/
- Gartner – several research papers, most by Paul Proctor
- Harvard Business Review:

Visuals: www.visualizevalue.com; Twitter @visualizevalue
Questions
What makes a good outcome driven metric?*

**Protect:** Measures a direct line of sight to a protection level.

**Coverage:** Measures the amount of coverage for a control.

**Strength:** Measures the strength of a control. Some controls can be tuned higher or lower depending on the needs of the organization.

**Benefit:** Measures the number of incidents related to the control.

**Blind:** Measure where there is no visibility into the state of a control or levels or protection.

**Friction:** Measures the business friction the control creates.

*According to Gartner*