PWNDEFEND

Cyber Security Leadership Slide Examples

Version 1.0

PUBLIC
www.pwndefend.com
Created by @UK_Daniel_Card

Dan’s Cyber Thought Hierarchy

Cyber Security Realities, 2022

PWNDEFEND

Most orgs don't have a security budget	Most orgs don't have a CISO	Most orgs don't have a SOC	MSPs generally don't have security specialists
Outsourced SOCs generally doesn't work well	Execs focus on tools rather than people	There is a skills gap!	Supply chain assurance questionnaires are commonly not accurate
People still misrepresent their security capabilities	Security is NOT a priority for many orgs	Most postures are weak	We still have lots of work to do!

CISO - First 100 Day Activities

PWNDEFEND

Learn the business landscape and make connections	Understand the financial landscape, build a business case & secure budget	Learn the people, skills, capabilities and gaps	Develop a business architecture view
Attack Surface Model from an Internet Facing Perspective	Understand the supply chain	Conduct an internal asset discovery	Develop an enterprise risk appetite statement
Do a maturity assessment and control mapping	Crown jewels analysis and threat modelling	Create cyber security roadmap	Improve something

Business Value Stream

Corporate Cyber Risk Management

PWNDEFEND

What is risk in relation to revenue? (current and future potential)	What legal risks are there?	What are the contractual obligations?	What does the threat landscape look like?
What political risks are likely in the near future?	What are the future business plans and where are the risks to these?	How do business resilience plans stack up against likely cyber incidents?	What historic incidents have occurred?
Where are the key business assets? What are the supply chain risks?	Do our security capabilities align to defending against likely risks?	Are the team aware of the cyber risks?	Are we covered for a “bad day” scenario?

Business Landscape

What do we sell?	Who are our customers?	What is the split of revenue by LOB delivery stream?	Who are the key stakeholders? What does the business org look like?
What is our business risk governance approach?	What's in the current risk registers?	Do the risk registers reflect the business architecture?	Who are the key suppliers?
Are there future business changes on the business roadmap that may fundamentally alter the landscape?	What are the business mission, vision, goals and objectives?	What does the business cost/opportunity portfolio look like?	What budget do we have for cyber security?

Threat Landscape

Human	Environmental	Social, Economical, Political, Legal
Nation State	Natural Disasters	Legal
Serious Organised Cyber Crime/Cybercrime	Physical/Facilities	Regulatory
Cyber Terrorists	Infrastructure	Political
Hacktivist/Lone Wolf		Economics
Malicious Insider/Supply Chain Malicious Insider		
Human Error		

Cyber Value Enablers

Reduce/Manage Risk	Gain competitive advantage in the marketspace	Cyber as a USP	Cost Optimisation
Business Intelligence through CYBER INTELLIGENCE	Reduce compliance costs	Increase market attractiveness	Demonstrate supply chain assurance
Democratise Cyber	Reduce likelihood and impact of incidents	Cyber as a business enabler/Cyber as a Customer Product	Business Portfolio Intelligence