CYBER SECURITY GOVERNANCE:

LATEST TRENDS, THREATS AND RISKS: JUNE 2019

CYBERSECURITY MATURITY MODELLING

Paul Forrest, Purple Management Consultancy

@HelloPurpleIC #cybersecurity @PDForrest

Purple
Delivering
Transformation
Together

> ” There are only two types of companies: Those that **have been hacked**, and those **that will be**.

Robert Mueller, FBI Director, 2012

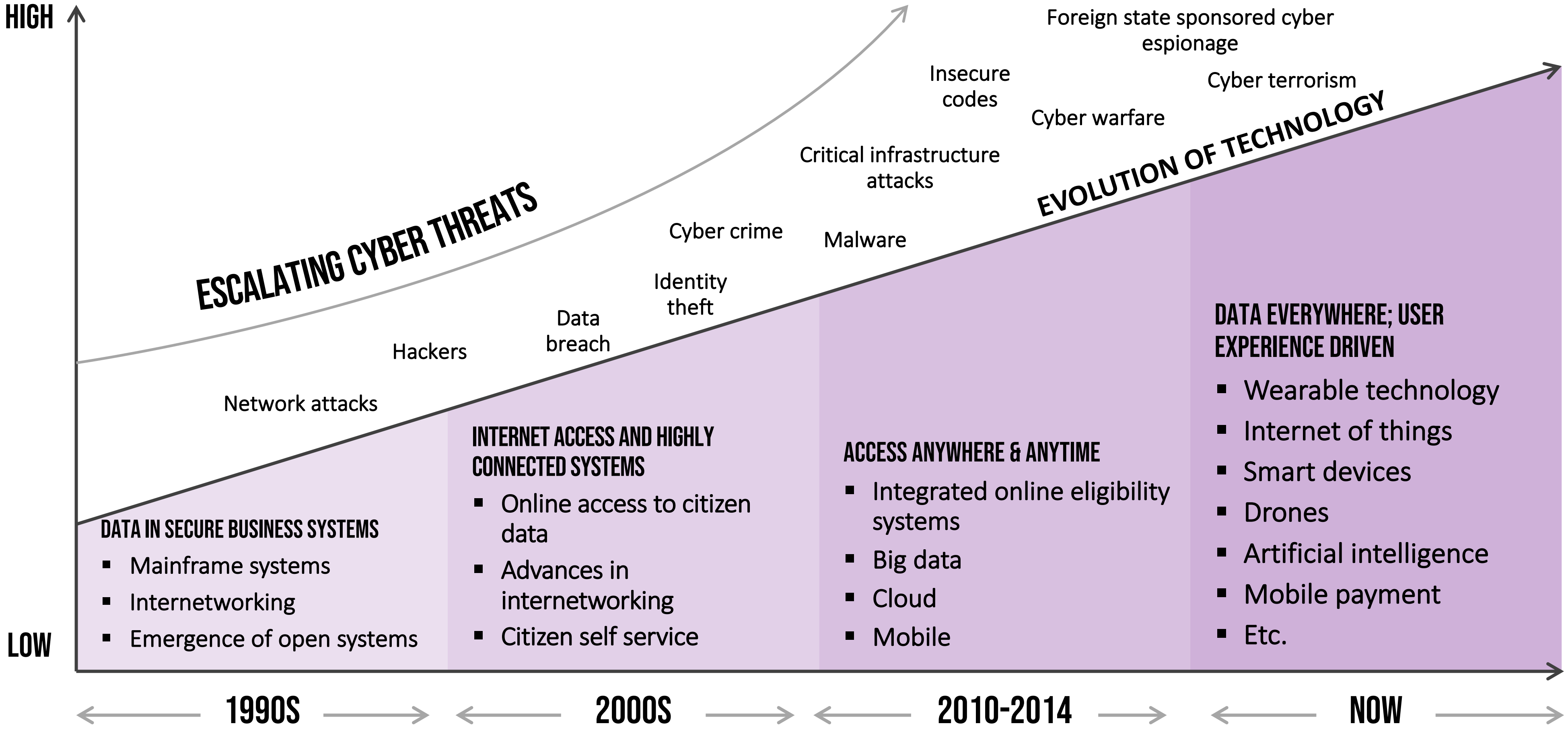
Purple
Delivering
Transformation
Together

THREATS

Complexity of Cyber Attack Capabilities are Growing

BUSINESS IMPACT:

- Trust
- Cost to protect
- Legal/ regulatory
- Critical infrastructure



HIGH

LOW

ESCALATING CYBER THREATS

Network attacks

Hackers

Data breach

Identity theft

Cyber crime

Malware

Critical infrastructure attacks

Insecure codes

Cyber warfare

Foreign state sponsored cyber espionage

Cyber terrorism

EVOLUTION OF TECHNOLOGY

DATA IN SECURE BUSINESS SYSTEMS

- Mainframe systems
- Internetworking
- Emergence of open systems

INTERNET ACCESS AND HIGHLY CONNECTED SYSTEMS

- Online access to citizen data
- Advances in internetworking
- Citizen self service

ACCESS ANYWHERE & ANYTIME

- Integrated online eligibility systems
- Big data
- Cloud
- Mobile

DATA EVERYWHERE; USER EXPERIENCE DRIVEN

- Wearable technology
- Internet of things
- Smart devices
- Drones
- Artificial intelligence
- Mobile payment
- Etc.

1990S

2000S

2010-2014

NOW

Purple
Delivering
Transformation
Together

THREATS

Attacker Classification

	ATTACKER	OBJECTIVE	MEANS	APPROACH
AIM	STATE ACTORS, INTELLIGENCE	Information Espionage Combat crime Damage	Enormous financial possibilities Benefits more important than costs	Buy knowledge Training Inconspicuous attacks Sustainable
	TERRORISTS	Damage Attention Political manipulation	Average financial means	Buying knowledge on the black market Physical and mental attacks
OPPORTUNISTIC	ORGANISED CRIME	Money	Business Earn money Focus: cost benefits	Existing gangs Organised specialists Blackmail
	HACKTIVISTS, GROUPS	Attention Damage Highlighting system vulnerabilities	Minimal means Huge bandwidth and coverage	Motivated amateurs & specialists Momentum
	VANDALS, SCRIPT KIDDIES	Fame Reputation Attention	Minimal means Little knowledge	Applying available tools

Purple
Delivering
Transformation
Together

SECURITY PLANNING

CYBERSECURITY PRACTICAL STEPS

Purple
Delivering
Transformation
Together

CYBER MATURITY – DISPEL THE MYTHS!

Cybersecurity Myths

WE CONDUCTED AN INTRUDER TEST.

The test should cover the entire infrastructure so that the company can quickly eliminate all discovered vulnerabilities.

WE'VE NEVER BEEN ATTACKED SO OUR SECURITY SYSTEM MUST BE GOOD.

Caution: threats continue to grow and become more complex.

WE'VE DESIGNED HIGH-END SECURITY TOOLS.

Security tools are only effective when properly configured, integrated and controlled within all security operations.

WE COMPLY WITH INDUSTRY REGULATIONS AND BEST PRACTICES.

Compliance requirements often only meet the minimum safety measurements and not all critical systems and information.

A THIRD PARTY PROVIDER RUNS OUR SECURITY.

Regardless of the competence and capabilities of the provider, the question is whether complex threats in a company will be taken seriously enough for a third party to sufficiently protect it.

WE'VE INVESTED IN STRICT SECURITY CONTROLS.

It is not enough to rely on standard IT security controls alone. Critical business elements should be above all protected.

OUR SECURITY IS MANAGED ADEQUATELY BY THE IT TEAM.

A threat can take over an entire business. Therefore, management should work closely with IT.

WE ONLY NEED TO SECURE OUR INTERNET APPLICATIONS.

One should also be equipped against internal threats and member/ staff abuse.

WE'VE COMPLETED OUR SECURITY PROJECT.

Security is an ongoing project that can never be completed.

WE AREN'T STATISTICALLY AT RISK.

Every company is at risk for a data breach and should be prepared.

Purple
Delivering
Transformation
Together

SECURITY PLANNING

Four Steps to Improve Cybersecurity

BE PREPARED	▪ monitor ▪ plan and test ▪ respond ▪ insure	SECURITY THROUGH PROTECTION AND RESILIENCE
SET THE BAR	▪ establish a risk-based and business-aligned strategy ▪ identify and protect valuable assets ▪ align architecture and capability	SECURITY THROUGH STRATEGY AND ALIGNMENT
GET THE BASICS RIGHT	▪ set access protocols ▪ conduct regular patching and manage vulnerable files ▪ secure essential systems ▪ Conduct regular testing and root cause analysis	SECURITY THROUGH CONTROL
PERSONAL PROTECTION	▪ develop security awareness ▪ lead from the top ▪ show consequences of poor behaviour ▪ include security practices at home	SECURITY THROUGH BEHAVIOUR

Purple
Delivering
Transformation
Together

SECURITY PLANNING

Tips for Implementing a Cybersecurity Program

FOCUS ON CRITICAL INFORMATION	What effect does an attack on your business have and what can be done about it?
EVALUATE A CYBER INCIDENT RESPONSE PLAN	What vulnerabilities have been identified and how have they been resolved?
LOOK OVER THE BUDGET	Is the cybersecurity budget being used appropriately?
BE INFORMED ABOUT KEY RISK INDICATORS	Do you know enough about defence, monitoring, risk and data protection?
WORK WITH INTERNAL AND EXTERNAL SPECIALISTS	Are you constantly being briefed on new developments in technology and cybersecurity?
FOLLOW THE SAFTEY RULES OF EXTERNAL PROVIDERS	What are the privacy and security policies of external providers? Do they meet your requirements?
COMPLY WITH LAWS/ REGULATIONS FOR CYBERSECURITY	Are you keeping up-to-date with the latest cyber threats and new laws?

Purple

Delivering
Transformation
Together

SECURITY PLANNING

The Basic Considerations

SECURITY GOVERNANCE AND MANAGEMENT	Policy & standards, strategy & operating model, risk management, training & awareness, third party security, physical security, business continuity, business engagement, metrics & reporting, asset management, human resources security
THREAT AND VULNERABILITY	Threat intelligence, vulnerability management, compliance monitoring, security incident management, penetration testing, event response and investigation
ACCESS AND IDENTITY MANAGEMENT	Provisioning & deprovisioning, user management, role based access control, multi factor authentication, access certification. FORCE REGULAR PASSWORD CHANGES.
APPLICATIONS	Secure system devices, code review, developer training, application protection, cloud protection
INFRASTRUCTURE	Security architecture, malware protection, web and email security, network protection, security hardening
DATA	Privacy, data classification, data protection, data back-up and availability, data discovery and monitoring, mobile device security. TAKE REGULAR BACKUPS AND TEST THEY WORK.

Purple
Delivering
Transformation
Together

DO NOW CHECKLIST

PRACTICAL CYBERSECURITY

Purple
Delivering
Transformation
Together

A SIMPLE MODEL FOR CYBERSECURITY MATURITY

	Embryonic	Developing	Established	Managed	Optimised
Governance, Policies & Awareness	Limited knowledge & basic leadership. Treated as an IT issue	Early stage risk assessments & basic security policies	Regular risk assessments, basic security planning and ad-hoc training	Regular policy reviews, comprehensive training & Compliance Monitoring	Progressive use of Trust, Privacy & Security as a Differentiator
Identity Management & Access Controls	Few Basic Alerts (OOB Configuration)	Limited Access Restrictions, early stage processes	Established/documented Management Practices	Suite of Analytics and Realtime Visualization	Comprehensive/predictive analytics based on Threat Landscape
Systems & Applications	Inconsistent Approach & Basic Automated Updates	Some Automated Patching and Application Self Reporting	Rules Based Patching Strategies and Basic Endpoint Security	Comprehensive Endpoint Security and Patch Management Strategy	As Managed with Strong Vendor Collaboration for Patching Risk Management
Monitoring & Detection	Basic Monitoring, No Alerts	Few Basic Alerts (OOB Configuration)	Basic SEIM & Continuity Planning	Integrated SEIM Tools with regular review and testing.	Rule based SEIM with detailed escalation procedures
Network Security	Basic Firewalls	Dedicated Firewalls & DMZs	Network Isolation & Tiered Firewalls	Centralised control and monitoring of Firewalls	Machine Learning and AI based Firewall Technology
Physical & Asset Security	Basic Procedure Documented	Basic Asset Inventories and Poor Physical Controls	Some testing of Physical Controls. Appropriate IT Asset Management	Good Configuration Management Practices & Strong Physical Controls	Physical Controls Regularly Tested and Asset Inventory Tested & Validated

Purple

Delivering Transformation Together

DO NOW CHECKLIST

Practical Cybersecurity Checklist

CYBERSECURITY CHECKLIST

Can you answer these questions about your business?

What is our plan to respond to a data breach?

How do we monitor our systems and prevent breaches?

How often do we verify the effectiveness of our security?

Is our security clear and consistent?

Are third parties really securing our most valuable information?

Do we treat cybersecurity as a business or an IT responsibility?

Are we adequately insured?

Do our security goals align with business priorities?

How much is the issue of security integrated into your business?

Do we have the basic rights for security measures?

Have we identified and protected our most valuable processes and information?

Purple
Delivering
Transformation
Together

ANY QUESTIONS?

Purple Management Consultancy

hello@purpleconsultancy.com

DISCLAIMER: This is non specific guidance designed to provide a background and appreciation for key GDPR tenets. You are advised to study the regulation and explore compliance issues pertinent to your own organisation

@HelloPurpleIC #cybersecurity @PDForrest

Purple
Delivering
Transformation
Together