CYBER RESILIENCE IN THE CASINO GAMING SPACE

PRESENTED BY: RMC LEGAL

December 13, 2018

DISCLAIMER

"The contents of this presentation are presented for general informational purposes only, and not for the purpose of providing legal advice. You should not consider any information provided to be legal advice and should not act upon any such information without seeking professional counsel. Use of this material or your attendance at this seminar does not create an attorney-client or any other relationship with the moderators, speakers, or panelists."

STATE ASSOCIATION SUPPORTERS:

REMINDER

To help facilitate efficiency and respect for your time, all participants will be on mute during the duration of today's event.

If at any time you would like to submit a question, you may type it into the "Questions" box on the right side of your screen, and these will be assembled and addressed via a follow up email to attendees. Additionally, questions may be submitted at info@casinowebinar.com

MODERATOR

Robert R. Russell
Gaming Analyst
Regulatory Management
Counselors, P.C.

RMC assists businesses in navigating the legal, regulatory and financial systems governing commercial and tribal casino industries. RMC Legal also assists businesses with numerous compliance matters, including the review of company policies related to security and regulatory compliance.

Robert Russell is a governmental and business consultant whose practice primarily focuses on the casino gaming industry. Russell is an active member of the American Gaming Association, Association of Gaming Equipment Manufacturers, as well as the State Gaming Coalition. Russell attended Michigan State University.

www.rmclegal.com

SPEAKERS

Tracy L. Lechner, Esq.*
Law Offices of Tracy L. Lechner LLC
tracy@tracylechnerlaw.com
646.872.8594

*Admitted in CO, CT and NY only.

Tracy L. Lechner founded the Law Offices of Tracy L. Lechner LLC in April, 2018. Prior to opening her own practice, Lechner led a prominent law firm's Cybersecurity and Technology Transactions, Licensing, Advanced Media and Privacy practice groups. Lechner has served as chief privacy officer, vice president and assistant general counsel to a multi-billion dollar media company, where she interfaced with business teams and senior management to identify and mitigate risk, ensure awareness of "best practices" on data privacy and data security issues and to develop strategic plans for the collection, use and sharing of data.

Lechner has also worked as Assistant Corporate Counsel for a digital advertising network owned by another major media conglomerate, providing strategic business and legal advice in connection with its online advertising, privacy and data collection practices. With more than a decade of in-house experience, Lechner has a unique, inside understanding of the complexities that organizations face in monetizing their data and protecting their assets. Lechner is a member of the International Association of Privacy Professionals ("IAPP") and is accredited by IAPP as a certified information privacy professional in the United States (CIPP/US). She serves as the co-chair of Denver/Boulder International Association of Privacy Professionals (IAPP) KnowledgeNet and is an Adjunct Professor at the University of Colorado School of Law.

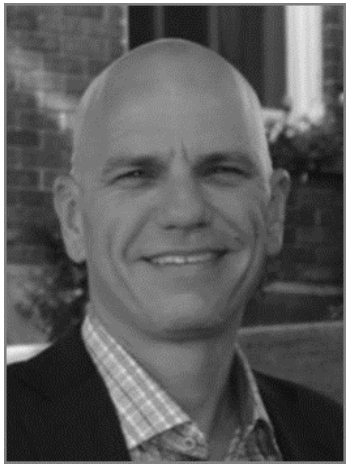
SPEAKERS

Maureen Kaplan, CISSP, GSLC
Global Head of Sales
Cloud & Security
Vodafone Business
Mobile: +44 7900 202272
maureen.kaplan@vodafone.com

Maureen Kaplan has over 18 years of cybersecurity leadership experience, working with organizations to help build their cybersecurity capability, understand the threat landscape and address the risks to their business. She is actively involved in digital transformation projects to evolve legacy systems and embrace new digital ways of working with a focus on “disruptive” ideas. Prior to joining Vodafone, Maureen was Chief Operating Officer for Verizon’s global Managed Security Services.

Kaplan is a frequent presenter to c-level executives on cyber security and effective business risk mitigation strategies. Maureen holds an engineering degree from the University of Michigan, is a Lean Six Sigma Black Belt, and holds Certified Information Security Systems Professional and GIAC Security Leadership Certifications.

SPEAKERS



Ryan Guzal, CISSP, CISM
Technical Consultant
RMC Cyber | InterLAN Security
phone: 248-820-7767
guzal@rmccyber.com

Ryan Guzal is an information security professional with nearly 25 years experience assisting clients secure corporate infrastructures, implement cyber programs and achieve digital compliance. He recognizes the need for a radical shift in the way businesses view and consume cyber services. Ryan strives to understand the unique challenges his clients face and help them mitigate risk through sustainable solutions.

Guzal is a graduate of Michigan State University, a Certified Information Systems Security Professional (CISSP) and a Certified Information Security Manager (CISM). An emergent strategist, Ryan has consulted with organizations large and small to help them better understand and adapt their digital landscape to align with changing business needs.

WEBINAR OVERVIEW

1. Overview of the Cybersecurity Legal and Regulatory Environment

2. Review Cyber Readiness and Awareness of Risks

3. Call to Action – Understand your organization's Security Maturity and path to Cyber Resilience

CYBERSECURITY: THE REGULATORY ENVIRONMENT

AN OVERVIEW FOR THE GAMING INDUSTRY

Presented By:

Tracy L. Lechner. Esq.

US REGULATORY ENVIRONMENT (FEDERAL)

US has a patchwork framework that is largely structured around industry.

1. **Gramm-Leach-Bliley Act** requires financial institutions to protect the security and confidentiality of customers' personal information. Unauthorized access to sensitive customer information requires an investigation and prompt notification of affected customers.

2. **Securities and Exchange Commission (SEC)** uses its civil law authority to bring cybersecurity-related enforcement actions to protect investors, hold bad actors accountable and deter future wrongdoing.
    - SEC guidance calls on public companies to be more forthcoming in disclosing cybersecurity risks even if no breach has occurred and warns corporate insiders not to trade shares based on cybersecurity issues that are not public yet. The guidance stresses the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents.

© Law Offices of Tracy L. Lechner LLC

US REGULATORY ENVIRONMENT (STATES)

Various states have regulations in place addressing the protection of financial and consumer information. California is recognized as having some of the most robust legislation.

California Consumer Privacy Act Effective: January 1, 2020	Creates a private right of action for consumers whose personal information "is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.
	Extraterritorial Reach – applies to any for-profit business that (1) "does business in the state of California"; (2) collects consumers' personal information and alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information; and (3) satisfies one or more of the following: (i) has annual gross revenues in excess of $25 million, (ii) annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households or devices, and/or (iii) derives 50 percent or more of its annual revenue from selling consumers' personal information. (Consumers are natural persons who are California residents)
	Data handled pursuant to GLBA is exempt.
California Data Breach Report 2016 published by Kamala D. Harris (fmr. Attorney General California Department of Justice)	All organizations that collect or maintain personal information should meet all 20 controls in the Center for Internet Security's Critical Security Controls. **The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.**
	Organizations should use multi-factor authentication to protect critical systems and data, and should also make it available on consumer-facing online accounts that contain sensitive personal
	Organizations should consistently use strong encryption to protect personal information on laptops and other portable devices and should consider it for desktop computers.
	Organizations should encourage individuals affected by a breach of Social Security numbers or driver's license numbers to place a fraud alert on their credit files and make this option very prominent in their breach notices.

US REGULATORY ENVIRONMENT (STATES)

In the US, 50 states (plus Washington, D.C., Puerto Rico, Guam and the U.S. Virgin Islands) have data breach notification laws)

Each state law has its own deadlines and requirements

- States have different definitions for what data constitutes "personal information"
- Some states require alternative means of notice when direct contact information is unavailable
- Some states require notification of residents based upon "unauthorized access"
- Some states require a risk of harm analysis
- Some states protect electronic records, not paper records
- South Dakota requires companies to notify consumers of a breach within 60 days of discovery or face fines of up to $10,000 per day per violation.
- Alabama has a 45-day notification requirement and allows for fines of up to $5,000 per day.
- Other states, including Arizona, Colorado, Louisiana and Oregon, have amended their laws to address credit freezes, expand the definition of personal information and shorten notification deadlines.

US REGULATORY ENVIRONMENT (INDUSTRY REGULATION)

Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards that are applicable to all companies that accept, process, store or transmit credit card information and are designed to ensure a secure environment.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Source: https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

This chart provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents

REGULATORY ENVIRONMENT (ABROAD)

There are at least 91 countries with data protection laws

- **The EU General Data Protection Regulation (GDPR)** became effective as of May 25, 2018 and affects companies that collect or processes personal data from EU residents.
  - The law overhauls how data and privacy is regulated in the EU and imposes strict new requirements on any entity that collects or processes personal data from the EU.
  - Non-compliance can result in fines as high as 4% of a company's global revenue.
  - Any person who has suffered "material or non-material damage" as a result of a breach of GDPR has the right to receive compensation (Article 82(1)) from the controller or processor.

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
Principle 4.7: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information." Canadian courts have upheld extraterritorial application of PIPEDA to companies involved in the collection of personal information in Canada through the offer and provision of services to Canadians.

REGULATORY ENVIRONMENT FOR EUROPEAN UNION CITIZENS

EU: General Data Protection Regulation (GDPR)

- 72-hour data breach reporting requirement.
- Requires that companies who collect personal data from data subject implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:
    - the pseudonymization and encryption of personal data;
    - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    - a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- GDPR takes into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."
- Adherence to an approved code of conduct or an approved certification mechanism — as described in Article 40 and Article 42, can be used to demonstrate compliance.

DATA PROCESSING

The GDPR holds companies responsible for how they <u>AND</u> their third-party vendors and service providers process, use, and protect personal data.

- Data Controllers that contract with Data Processors must:
  - Describe what info will be processed, duration and purpose of the processing.
  - Establish the processor's responsibilities.
  - Maintain and exercise audit rights to verify the processor's compliance with contractual obligations and restrictions.
  - Clearly require the processor to comply with security obligations, maintain qualified personnel to protect data privacy, and respect the rights of data subjects (e.g., right of access and right to be forgotten).
  - Keep and require processors to keep records of data processing activities.

Due diligence, compliance oversight, and appropriate contractual provisions are key!

PRACTICAL STEPS TOWARDS COMPLIANCE

- **Data Mapping & Security Controls.** Determine what data is being collected, how it is being used, why it was collected, how, under what authority, how long it will be retained, how secure it is, and whether it is and/or should be shared with third parties. Identify and redress compliance gaps. Ensure that appropriate security controls are in place.

- **Review and update privacy notices.** Ensure that the company has a legal basis for collecting and processing personal information. Identify and address gaps between the company's data collection and processing practices and what the company has disclosed to data subjects. **Don't misrepresent what the company is doing.**

- **Update contracts, policies and procedures.** Ensure that company policies and procedures are up to date, that consumer contracts and contracts with service providers and vendors contain appropriate disclosures and requirements.

- **Employee Training.** Train employees at regular intervals on security best practices and on company policies and procedures to ensure that they are properly implemented.

- **Incident response preparedness.** Ensure that the company has adequate procedures in place to detect, report, investigate and mitigate a data breach.

ASSEMBLE EXTERNAL RESOURCES

OUTSIDE COUNSEL	Outside counsel can retain and oversee third party service providers to provide breach investigative and response services, advise on breach communications, and put a company in a better position to maintain privilege.
FORENSIC INVESTIGATORS	Forensic investigators can help identify the cause of a breach, mitigate the breach, and suggest measures to help prevent future breaches.
PR/GR FIRMS	Public relations firms and government relations firms can help manage the media coverage of and government/consumer perception of a breach.
CREDIT MONITORING	Identity theft protection and credit monitoring companies can offer better rates if approached before a breach occurs.
INSURANCE	Insurance companies can provide coverage and resources to help mitigate risk and liability.
CYBER ADVISERS	Outside consultants can offer additional industry expertise in identifying and mitigating risk.

Questions?

Tracy L. Lechner, Attorney & Founder *

Law Offices of Tracy L. Lechner, LLC

Tracy@tracylechnerlaw.com

646.872.8594

* *Admitted in CO, CT and NY only.*

CYBER READINESS
CYBER READY BAROMETER RESEARCH

Presented By:
Maureen Kaplan, CISSP, GSLC

THE CYBER READY BAROMETER RESEARCH

Objective: To assess security readiness across businesses and its affect on success

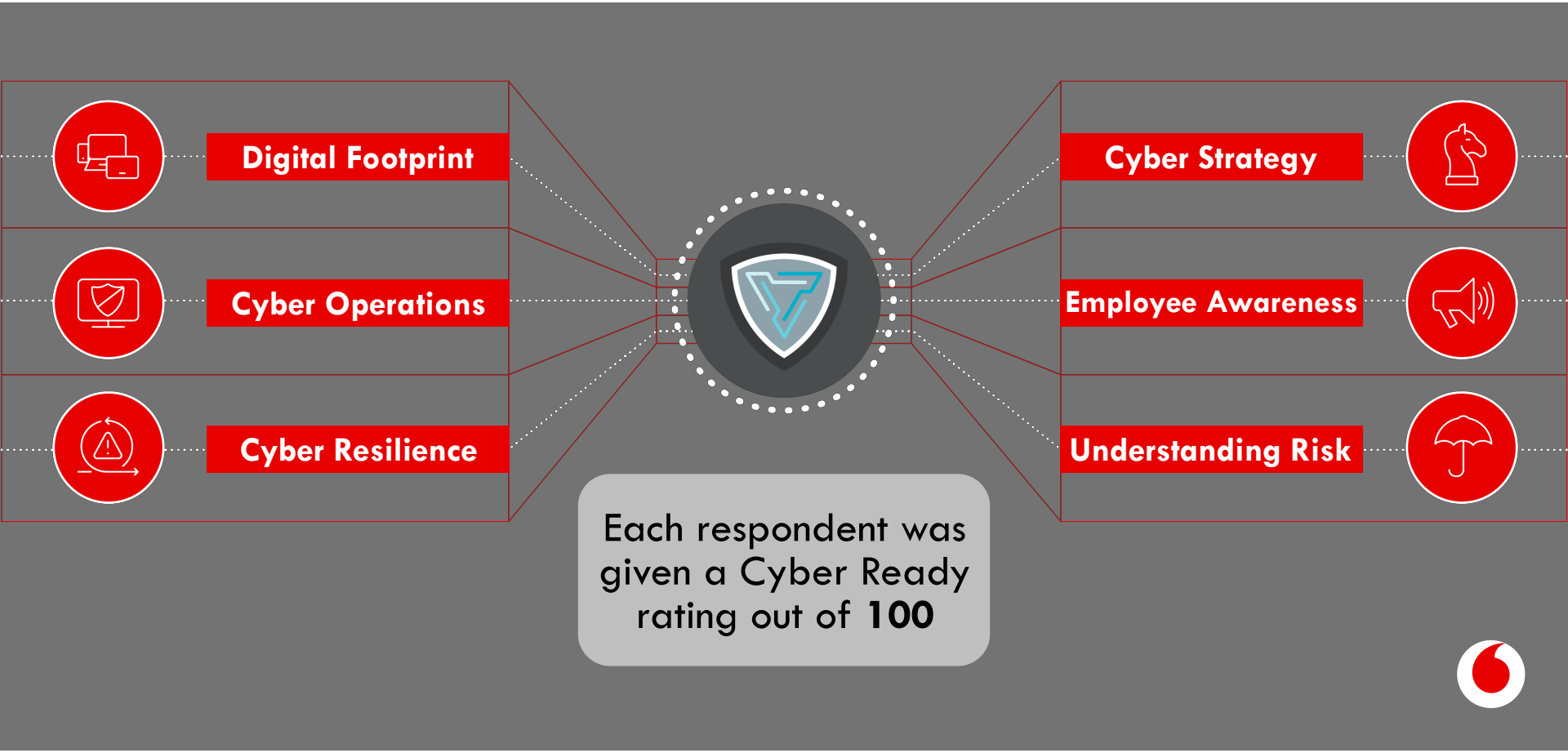
4,809 IT leaders, employees and consumers surveyed

Across **9** countries

and **8+** verticals including

- Technology & media
- Healthcare & Pharmaceutical
- Financial services
- Transport & logistics
- Retail
- Construction
- Public sector
- Manufacturing

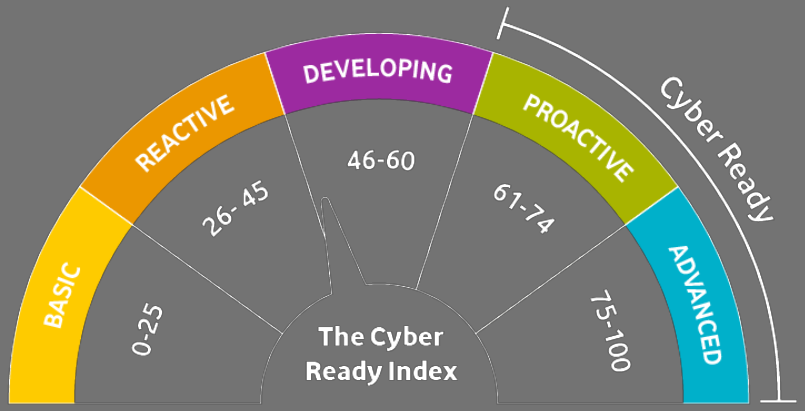
CYBER READY INDEX: SIX CRITERIA



FIVE LEVELS OF CYBER READINESS

46/100

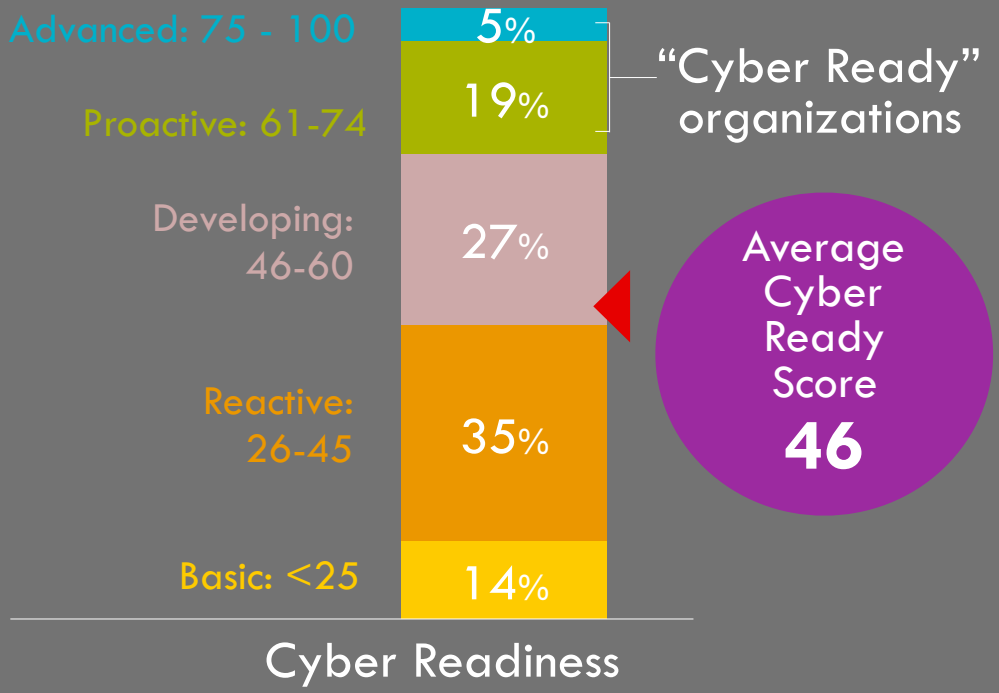
The average score across all businesses is 46 - Developing readiness.

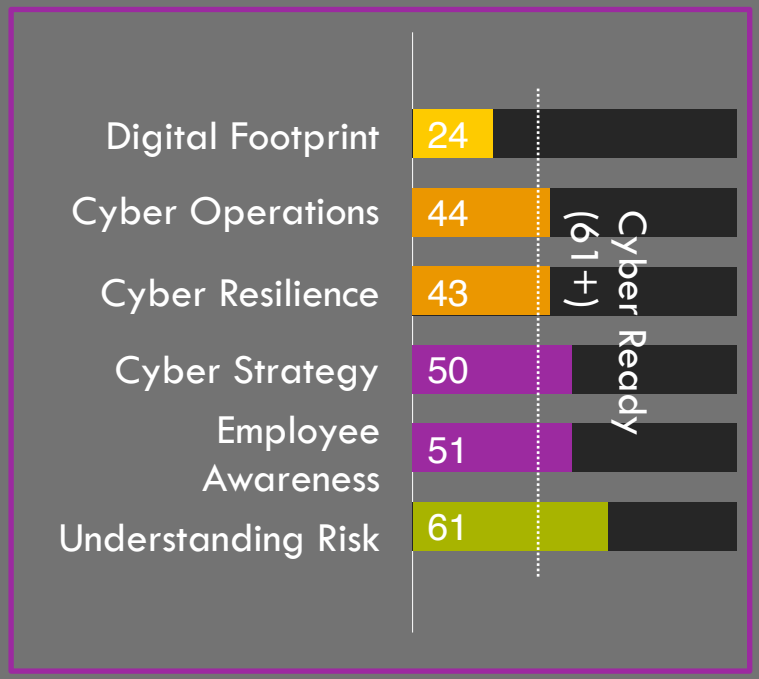


Only 1 in 4

businesses are Cyber Ready and larger firms are Ready than smaller businesses

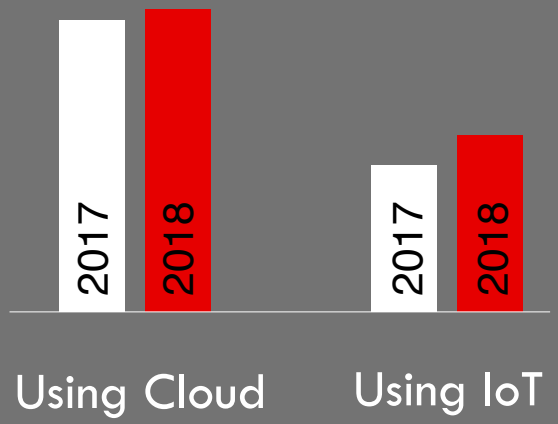
1. AWARENESS OF CYBER RISK IS INCREASING





2. CHALLENGE OF EVOLVING DIGITAL FOOTPRINTS

More businesses are using cloud services and IoT devices



The average consumer household uses

9 connected devices

11 online services

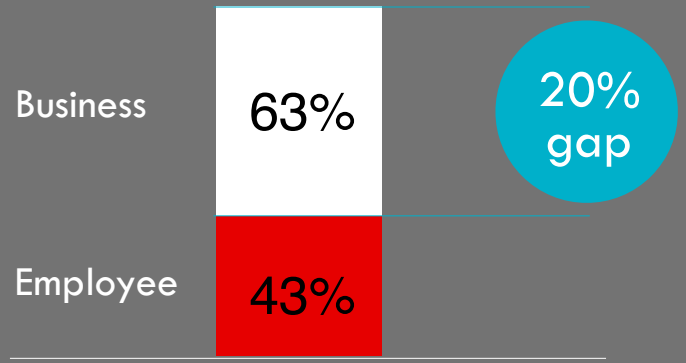
3. EMPLOYEES AND BUSINESSES HAVE DIFFERING VIEWS

Employee engagement needs more focus

47% said official policy is followed by all staff

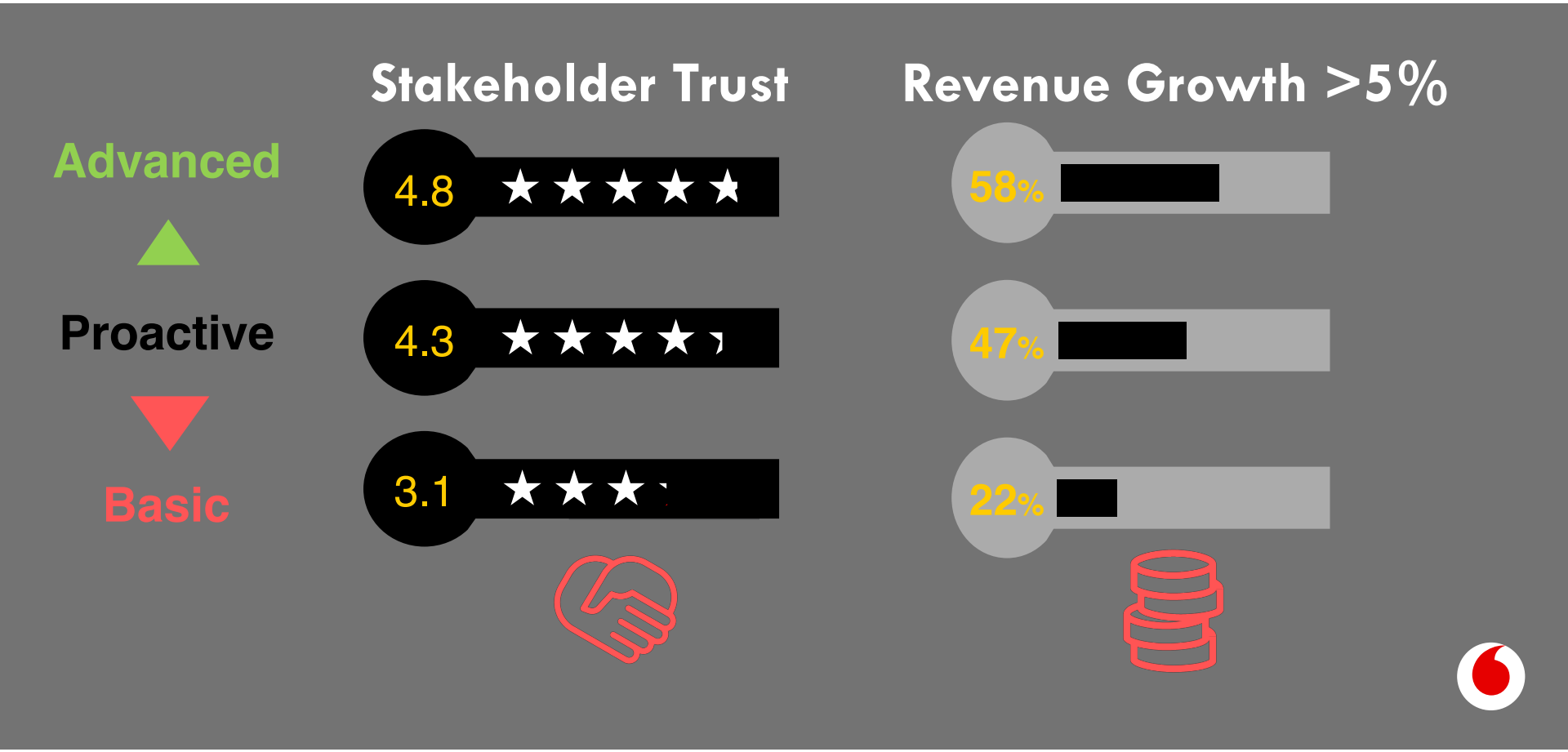
39% said security is a box-ticking exercise

Disconnects exist between decision-makers and employees



% staff using "bring your own device" (BYOD) for work

4. BUT THE MORE CYBER READY, THE BIGGER THE ADVANTAGE



5. THE CONSUMER SECURITY ADVANTAGE

70%
consider themselves at risk of cyber attack

43%
don't trust security measures of companies they use

63%
have stopped using an online service due to security concerns

59% of consumers would pay more for better security - but just 29% of businesses think they can charge more

Questions?

Maureen Kaplan, CISSP, GSLC

Global Cybersecurity Lead,
Vodafone Group

maureen.kaplan@vodafone.com
+44 7900 202272

UNDERSTANDING YOUR ORGANIZATION'S SECURITY MATURITY — *THE PATH TO CYBER RESILIENCE*

Presented By:
Ryan Guzal, CISSP, CISM

SITUATIONAL NOTES

Experts predict cybercrime damages will reach $6 Trillion for 2021*

**2017 Official Annual Cybercrime Report, Cybersecurity Ventures*

- Losses per incident cost in excess of $3 Million on average
- Industry facing a shortage of 3 Million resources globally in Information Security

Represents "the greatest transfer of economic wealth in history...will be more profitable than the global trade of all major illegal drugs combined."

Cybercrime is "not just about more sophisticated weaponry, it's as much about the growing number of human and digital targets." And bogeys.

SITUATIONAL NOTES

Data: The world's 'new natural resource'

"We believe that data is … the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true—even inevitable—then cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world."

-Ginni Rommety, President and CEO of IBM

"It is possible to do a good job at your security…and still get compromised."
-Troy Hunt

From Brian Krebs:

Reality #1: Bad guys already have access to personal data points that you may believe should be secret…including your credit card information, Social Security number, mother's maiden name, date of birth, address, previous addresses, phone number, and yes even your credit file.

Reality #2: Any data point you share with a company will in all likelihood eventually be hacked, lost, leaked, stolen or sold usually through no fault of your own. And if you're an American…your recourse to do anything about that…is limited or nil.

THE CAUSE: RAMPANT EXPOSURE & BREACHES

- **HSBC** password stuffing - “Hapless Security: Become Compromised” - estimated 1% or roughly 12,000 users
- **Pakistan** debit card breach - reported as “all banks” were hacked. It was actually credit card skimming - 20,000 users affected
- **Google+** - 50 Million users affected
- **Marriott** - 500,000,000 affected
- **India AmEx** - 700,000 users affected - unencrypted DB
- **Facebook** - 50 million users affected, lager found another 80,000+ via another hack.
- **Under Armor** - 150 million
- **Twitter** - 330 million
- **Cathay Pacific** - 9.4 Million

THE EFFECT: NO CARROT, NEW STICK

Casinos have some unique aspects:

- Vendor dependent with plug in systems – hotel, gaming systems, and this will expand with Free Play marketing sites and ultimately online gaming
- Data rich environments
- Public policy issues with gaming regulators

The regulators are coming:

"The SEC has identified public companies' failure to detect and mitigate effects of cyber fraud as a significant compliance issue warranting robust enforcement."

Gaming is not far behind:

- New Jersey's Division of Gaming Enforcement regulates that all gaming facilities in Atlantic City must have an information security officer.

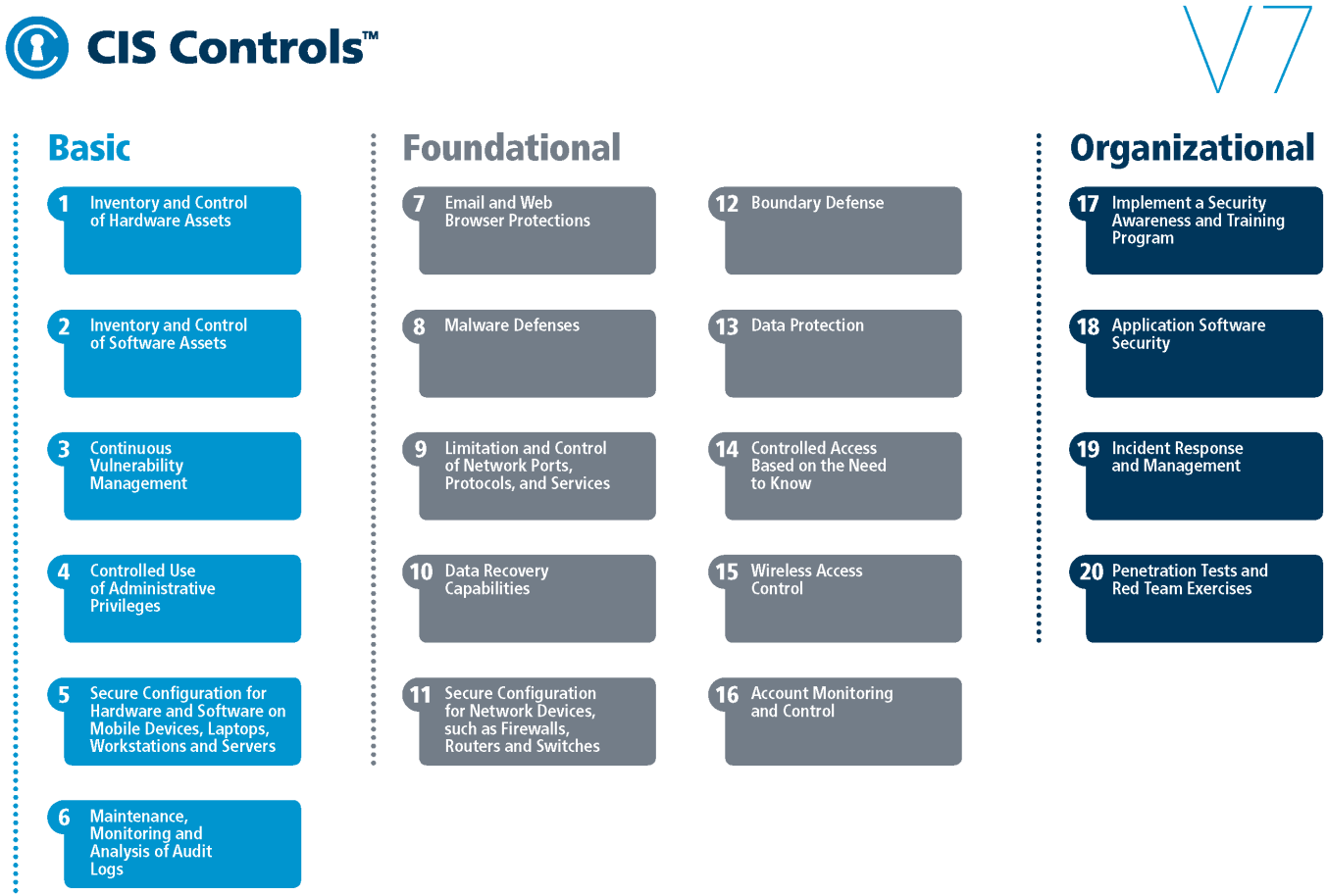
- GDPR mandates the appointment of a Data Protection Officer if, "your core activities require large scale, regular and systematic monitoring of (EU) individuals."

SECURITY MATURITY

	Basic Organizations	Progressing Organizations	Advanced Organizations
Philosophy	Cybersecurity is a "necessary evil."	Cybersecurity must be more integrated into the business.	Cybersecurity is part of the culture.
People	CISO reports to IT. Small security team with minimal skills. High turnover and burnout rate.	CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed and under-skilled.	CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good working environment. Skills and staff problems persist due to global cybersecurity shortage.
Process	Informal and ad-hoc. Subservient to IT	Better coordination with IT, but processes remain informal, manual and dependent upon individual contributors.	Documented and formal with an eye toward more scale and automation.
Technology	Elementary security technologies with simple configs. De-centralized security organization with limited coordination across functions. Focus on prevention and regulatory compliance.	More advanced use of security technologies and adoption of tools for incident detection and security analytics.	Building an enterprise security technology architecture. Focus on incident prevention, detection and response. Continual evaluation of new technologies and adding elements to deal with emerging threats and new usage patterns.

Source: Enterprise Strategy Group, modified

A LOOK AT CONTROLS



This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode

To further clarify the Creative Commons license related to the CIS ControlsTM content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to (http://www.cisecurity.org/controls/) when referring to the CIS Controls in order to ensure that users are employing the most up to date guidance. Commercial use of the CIS Controls is subject to the prior approval of CIS® (Center for Internet Security, Inc.).

THE PATH TO RESILIENCE

1. Establish a Security Program
    1. Understand your Risk (Risk Assessment / Register)
    2. Adopt a Framework
    3. Maintain a System of Internal Controls
    4. Work the Plan (build out and continuously reassess controls)

Credit: GDJ/Pixabay

THE PATH TO RESILIENCE

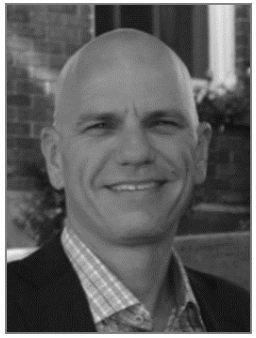
Credit: GDJ/Pixabay

2. Focus on the high impact areas
    1. Threat Vulnerability Management (patching, etc)
    2. Business Continuity/DR (backups)
    3. Access Management (especially Privileged Access)
    4. Third Party connections
    5. User Awareness Training

Questions?

Maureen Kaplan, CISSP, GSLC
Global Cybersecurity Lead, Vodafone Group
maureen.kaplan@vodafone.com
+44 7900 202272

Tracy L. Lechner, Attorney & Founder *
Law Offices of Tracy L. Lechner, LLC
Tracy@tracylechnerlaw.com
646.872.8594
* *Admitted in CO, CT and NY only.*



Ryan Guzal, CISSP, CISM
InterLAN Security | RMC Cyber
guzal@rmccyber.com
248.820.7767

Robert Russell
Gaming Analyst,
Regulatory Management Counselors, P.C.
russell@rmclegal.com
517.507.3858

Submit Your Questions

Info@casinowebinar.com

Recording of the Webinar will be made available at www.casinowebinar.com

RESOURCES

National Institute of Standards and Technology (NIST)
https://www.nist.gov/cyberframework

Security Program Primer
https://www.linkedin.com/pulse/security-program-idea-ryan-guzal/

CIS Risk Assessment Method
https://learn.cisecurity.org/cis-ram

Brian Krebs
https://krebsonsecurity.com/

HIBP
http://www.haveibeenpwned.com
Created by Troy Hunt, HIBP is a website that tracks breaches and individual email accounts that have been compromised.

Vodafone Cyber Ready Barometer
https://img.en25.com/Web/VodafoneGroupPLC/%7b1dd2abd4-17b9-4e81-9b23-347f2b41f338%7d_Vodafone-Cyber-Ready-Barometer-research-report-2018.pdf