/// Segurança da Informação – Tendências Actuais

Promovendo o Crescimento Azul - H2020 e Segurança Marítima
6 Novembro 2015

Bruno Morisson, Partner & Audit Services Director
MSc Information Security (RHUL), CISSP-ISSMP, CISA, OSCP, ISO 27001 LA

INTEGRITY

consulting & advisory

INTEGRITY

- ✓ Fundada em **2009** por **profissionais sólidos** e **experientes**.
- ✓ Focus em Consultoria e Auditoria em **Segurança da Informação.**
- ✓ Equipa dispõe de **notoriedade no setor** e **Certificações Internacionais** muito relevantes em Segurança da Informação.
- ✓ **HQ** em **Lisboa** e escritórios em **Londres**.
- ✓ A **maior** e **mais certificada equipa** de Segurança da Informação em Portugal a competir ao nível Global.

PERFIL DOS RECURSOS SENIORES

- ✓ Sendo uma empresa de serviços, o **foco** da prática da INTEGRITY é o ***know-how*, experiência e formação continuada dos recursos**.
- ✓ No âmbito da Segurança da Informação, dispomos de **recursos de excelência** com **mais de 12 anos de experiência** (média) em consultoria e gestão de serviços críticos, dispondo no seu conjunto de:

- ✓ **MSc** Information Security;
- ✓ **PG** Information Security;
- ✓ **OSCP** (Offensive Security Certified Professional);
- ✓ **CISSP** (Certified Information Systems Security Professional);
- ✓ **ISO 27001** Lead Auditor;
- ✓ **CISA** (Certified Information Systems Auditor).

ISO 27001 desde Abril 2012

- **Padrão e referência internacional** na **Gestão da Segurança da Informação**.
- O seu **princípio** é a adoção de um conjunto de requisitos, processos e controlos para **gerir adequadamente o risco da organização**.
- O **âmbito** da certificação foi a **proteção da informação de projetos de clientes**.

ISO 9001 desde Setembro 2014

- **Padrão e referência internacional** na **Gestão da Qualidade**.
- O seu **princípio** é a adoção de um conjunto, processos e controlos para **entrega de serviço com qualidade**.
- O **âmbito** da certificação foi **Consultoria, Auditoria e Assessoria em Segurança de Informação e Implementação de Sistemas de Gestão**.

CREST desde Novembro 2014

- **O CREST** é uma organização sem fins lucrativos e que garante standards e qualificações, reconhecidas pela Indústria e Governo, para empresas e profissionais cujo enfoque seja o fornecimento de serviços técnicos de segurança da informação.
- A **INTEGRITY é acreditada pelo CREST** no que concerne aos seus serviços de PenTesting, tendo sido sujeita a processo de certificação respectivamente às suas práticas tecnológicas e de gestão.

SOME OF OUR CLIENTS

Retalho

Aviação

Indústria

Energia

Organismos Públicos

Bancas & Seguros

Companhias de Serviço

Tecnologias de Informação

SOME OF OUR CLIENTS

A providenciar serviços

8 Países
3 Continentes

Auditing

- Área de negócio dedicada à realização de **Auditorias de Segurança da Informação**, nomeadamente Testes de Intrusão.
- A Integrity detém uma abordagem inovadora ao nível Global de **Testes Persistentes**, denominada de KEEP-IT-SECURE-24.
- Empresa **líder** em Portugal em **termos de serviços de PenTesting** em termos de equipa, projectos e certificações.

Consulting

- Área de negócio dedicada à prestação de serviços de **Consultoria em Segurança da Informação** com base nas **melhores práticas de Gestão** em Segurança da Informação.
- Experiência comprovada muito relevante na **implementação e suporte** do Standard Internacional **ISO 27001.**
- Avaliação da **Postura Global** de Segurança da Informação.

Managed Services / Awareness, Training

Serviços de **Gestão de Infra-Estruturas** de Segurança da Informação.

Formação e Consciencialização em Segurança da Informação (**Lisbon Security Academy**)

/// Tendências Actuais de Segurança da Informação

INFORMATION SECURITY in Late 90s / Early 2K

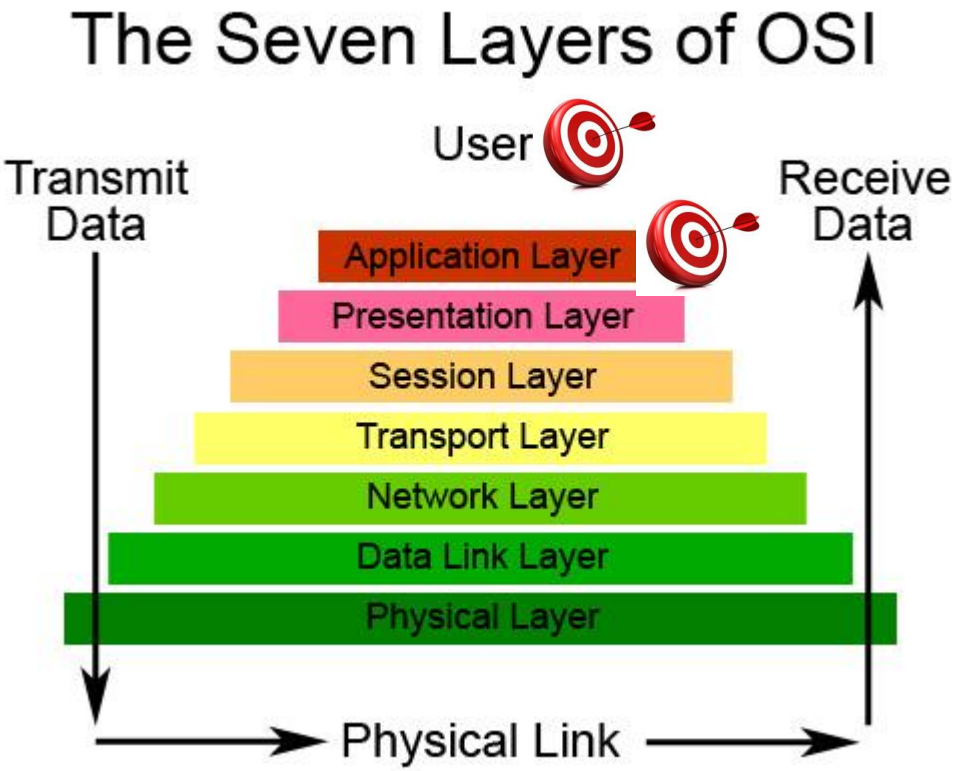
What's Happening?

What's Happening?

Ask Before…

What's NOT Happening!!!!!

Attack Sophistication



Mobile …

Cloud …

Internet of Things…

Social Media …

Regulations / Compliance / Laws …

Business Flexibility …

Cost Reduction…

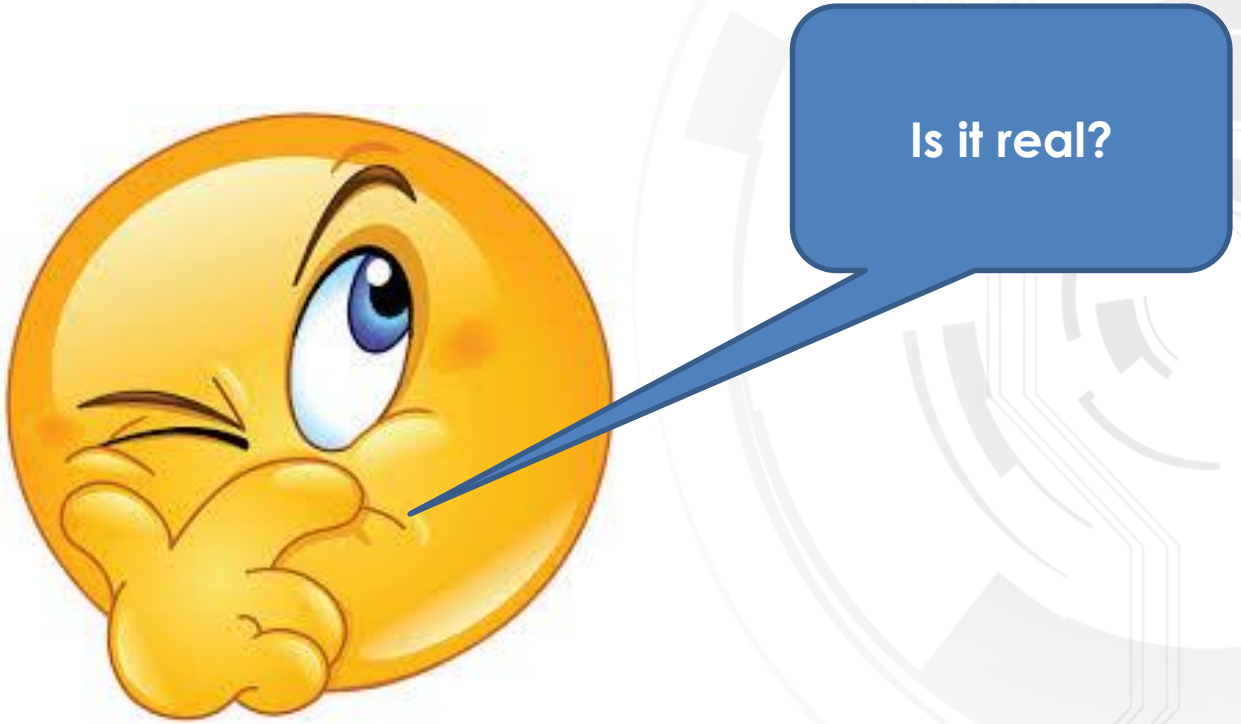
A conjuntura está a mudar radicalmente!!

INFORMATION SECURITY ??

Welcome to:

CYBERSECURITY 2.0

A conjuntura está a mudar radicalmente!!



Exemplos …

RTP NOTÍCIAS

INÍCIO EM FOCO PAÍS MUNDO POLÍTICA ECONOMIA CULTURA DESPORTO TRÂNSITO TEMPO IMA

RTP / Início / Vídeo e Áudio / País

Judiciária alerta para chamadas fraudulentas em nome da Microsoft

20 Fev, 2015, 13:46 / atualizado em 20 Fev, 2015, 14:20

A PJ está a investigar vários casos de fraude informática que têm por base chamadas telefónicas em nome da Microsoft. Quem telefona apresenta-se como funcionário do departamento de segurança de informática da Microsoft, fala em Inglês e diz que está a resolver problemas do computador pessoal de cada um.

88 +1 0 6 0

Corrigir
Leia-me
Imprimir
Enviar
Partilhar
Aumentar
Diminuir

Exemplos …

WIRED How Hackable Is Your Car? Consult This Han

ANDY GREENBERG 08.06.14 6:30 AM

HOW HACKABLE IS YOUR CAR? CONSULT THIS HANDY CHART

Stuart Dee/Getty

LAST YEAR, WHEN hackers Charlie Miller and Chris Valasek showed they could hijack the steering and brakes of a Ford Escape and a Toyota Prius with

www.wired.com/2015/04/hasbro-vimeo-on-demand/

Exemplos …

A Survey of Remote Automotive Attack Surfaces

By Charlie Miller (Twitter: cmiller@openrce.org)

& Chris Valasek (IOActive: cvalasek@gmail.com)

Contents

http://www.scribd.com/doc/236073361/Survey-of-Remote-Attack-Surfaces

Happening all the time…

Newsweek

Europe Edition Social

HOME WORLD BUSINESS TECH & SCI

TECH & SCIENCE

Sony Cyber Attack One of Worst in Corporate History

BY AMELIA SMITH 12/4/14 AT 6:14 PM

A magnifying glass is held in front of a computer screen in this picture illustration taken in Berlin May 21, 2013.
PAWEL KOPCZYNSKI/REUTERS

euobserver

Register Login

Cyber attack on French TV finds EU unprepared

The attack by the so-called CyberCaliphate disrupted all TV5 Monde channels and websites.

By ERIC MAURICE

BRUSSELS, 10. APR, 18:06

An attack on French TV channel TV5 Monde on Wednesday (8 April) highlighted Europe's vulnerability to high-tech cyber criminality.

Happening all the time…

Outside JPMorgan's corporate headquarters in New York. Andrew Burton/Getty Images

JPMorgan Chase

July-August 2014

The computer networks of JPMorgan Chase were infiltrated in a series of coordinated, sophisticated attacks that siphoned off gigabytes of data, including checking and savings account information.

JPMorgan Chase said account information of 83 million households and small businesses were compromised. Authorities said the same hackers tried to to gain access to the systems of at least a dozen other financial institutions.

In the JPMorgan attack, the bank said it found no evidence of any fraud or misuse of customer information. JPMorgan said the hackers got access only to customer email addresses, homes addresses and phone numbers but nothing of a more sensitive nature like Social Security numbers.

Outside a Staples store in Elmwood Park, Ill. Scott Olson/Getty Images

Staples

October 2014

The office supply retailer said hackers had broken into the company's network and compromised the information of about 1.16 million credit cards.

Happening all the time…

Obama declares cyberattacks a 'national emergency'

624 298 46 COMMENTS 30

Getty Images

By Cory Bennett and Elise Viebeck - 04/01/15 09:13 AM EDT

President Obama declared Wednesday that the rising number of cyberattacks against the United States is a national emergency and issued an executive order that would sanction those behind the attacks.

Happening all the time…

www.engadget.com/2015/10/23/talktalk-hacked/

engadget REVIEWS FEATURES GUIDES VIDEOS GALLERIES PUBLIC ACCESS GAMING ENGADGET LIVE

TalkTalk hacked in 'significant and sustained cyberattack'

by Matt Brian | @m4tt | October 23rd 2015 At 3:37am

TalkTalk subscribers are this morning waking up to news that the company has been the subject of another hack. Following an intrusion at the end of last year, which saw some customer data stolen, the broadband provider announced today that its website was the target of a "significant and sustained cyberattack" that may have captured personal details including names, addresses, account information *and* credit card/bank data.

Public Access

Happening all the time…

news.sky.com/story/1581329/fourth-person-bailed-over-talktalk-hack

We use cookies to give you the best experience. If you do nothing we'll assume that it's ok. Close

Switch to US Edition

sky NEWS Search Watch Live

Home UK World US Business Politics Technology Entertainment Strange News Weather More

Fourth Person Bailed Over TalkTalk Hack

The teenager is bailed until March after being detained in connection with a cyber attack on the company's computers.

10:30, UK, Wednesday 04 November 2015

TalkTalk's four million customers have been asked to check their accounts

A 16-year-old boy from Norwich has been bailed after being arrested in connection with alleged data theft from TalkTalk.

Top Stories

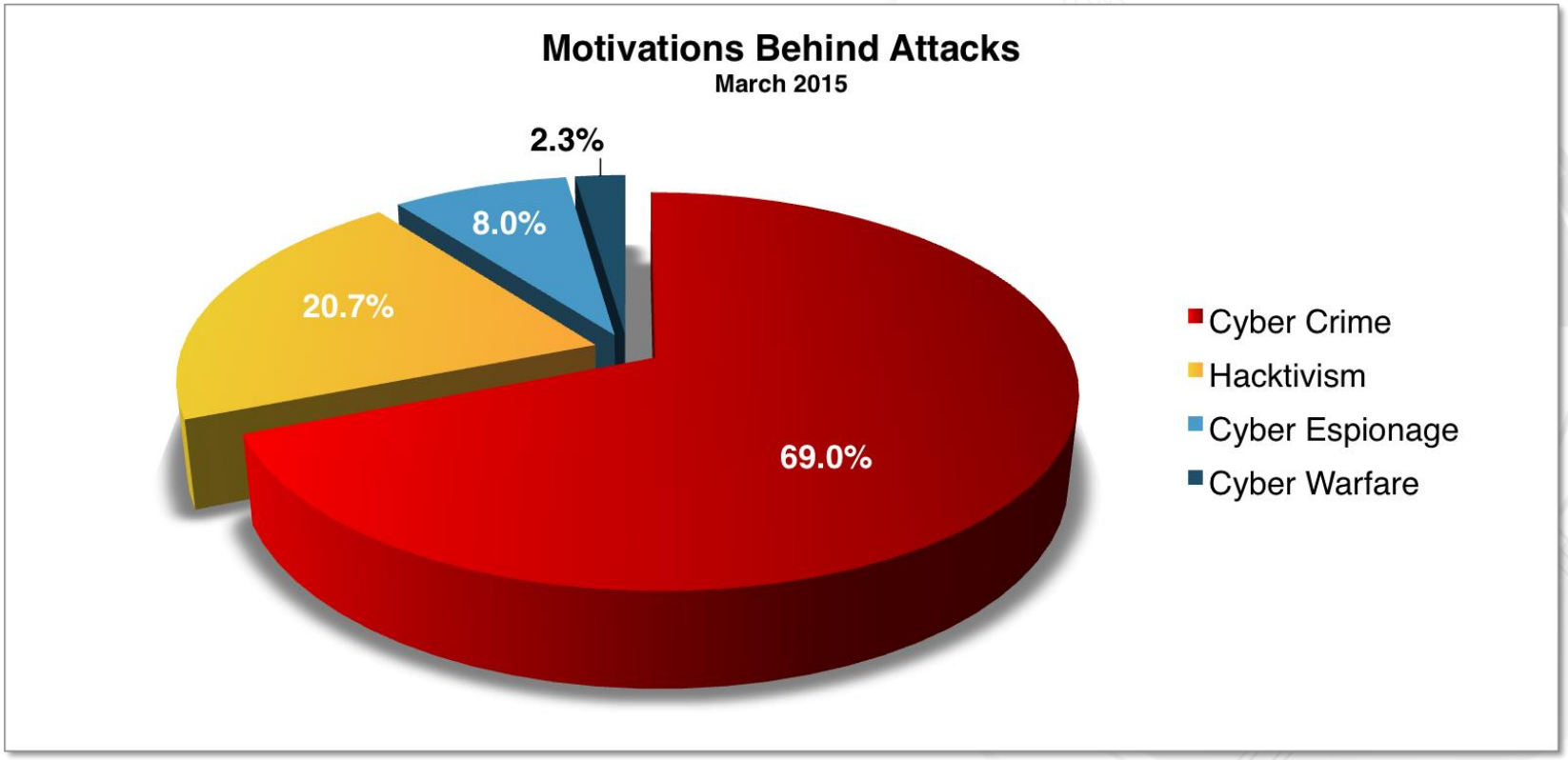

May: Spies To Get Access To Web History

Web Surveillance: What You Need To Know


Dozens Killed As Plane Crashes In South Sudan


Labour Leader Condemns Egypt President Visit

Motivations…



Source: http://hackmageddon.com/

Interesting Data…

Interesting Data…

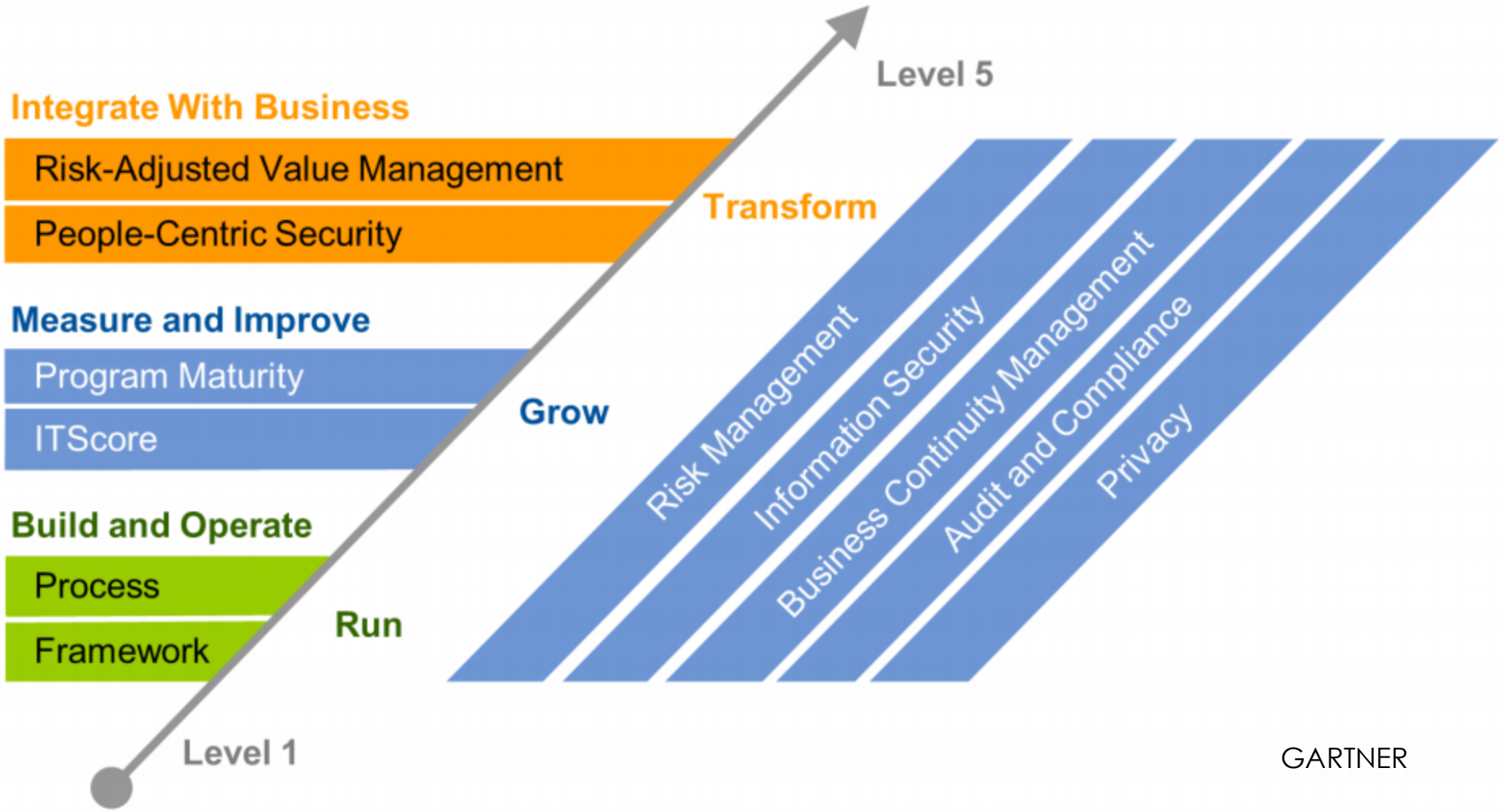
Scope:
741 Responsáveis pela Gestão da Segurança da Informação de organizações Líderes.

Questões:

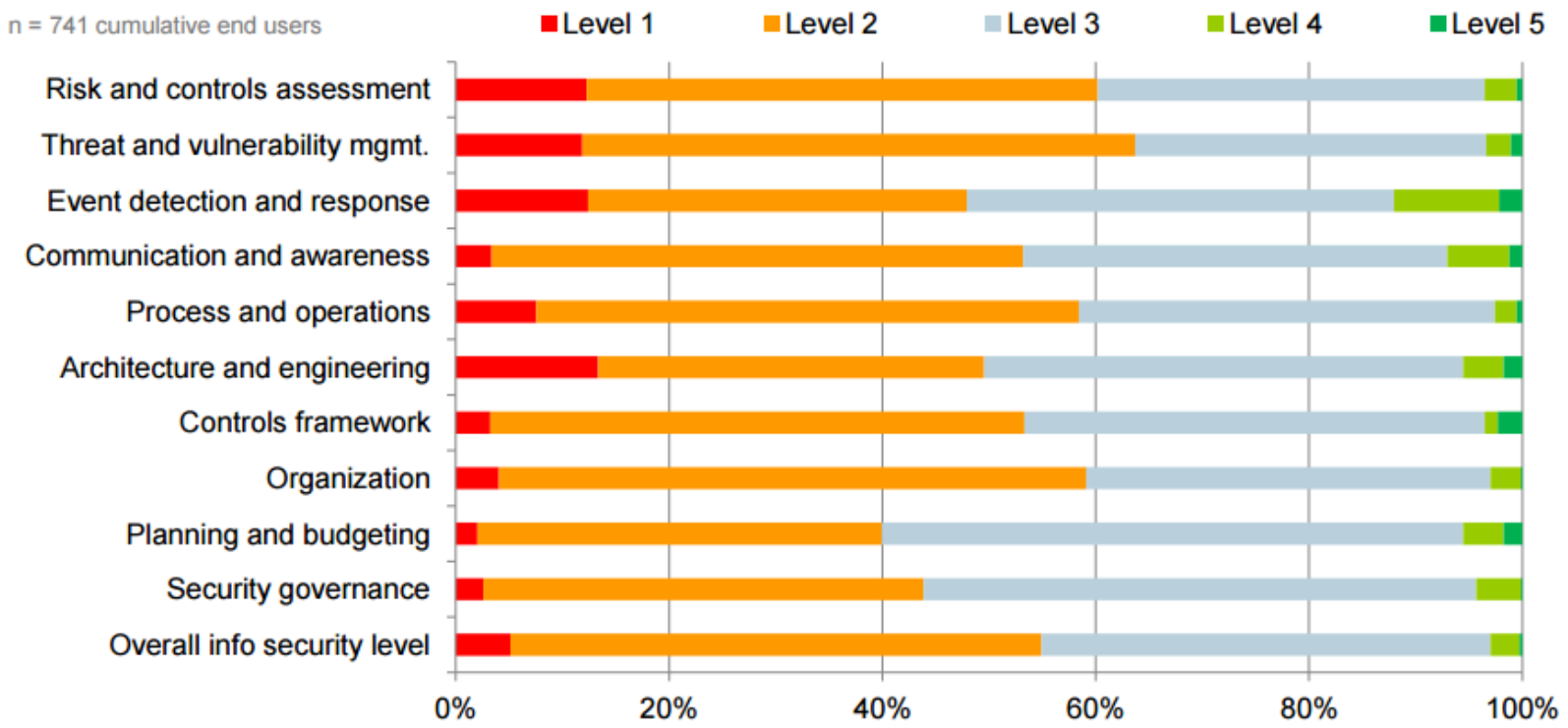
- Classificar o estágio de maturidade de um conjunto de áreas tecnológicas.
- O que estão adoptar em termos tecnológicos.
- Previsões sobre alterações no budget de Segurança da Informação.

- Cloud Risk Appetite Spectrum.

Source: Gartner


Level 5
Integrate With Business
Risk-Adjusted Value Management
People-Centric Security
Transform
Measure and Improve
Program Maturity
ITScore
Grow
Build and Operate
Process
Framework
Run
Level 1
Risk Management
Information Security
Business Continuity Management
Audit and Compliance
Privacy

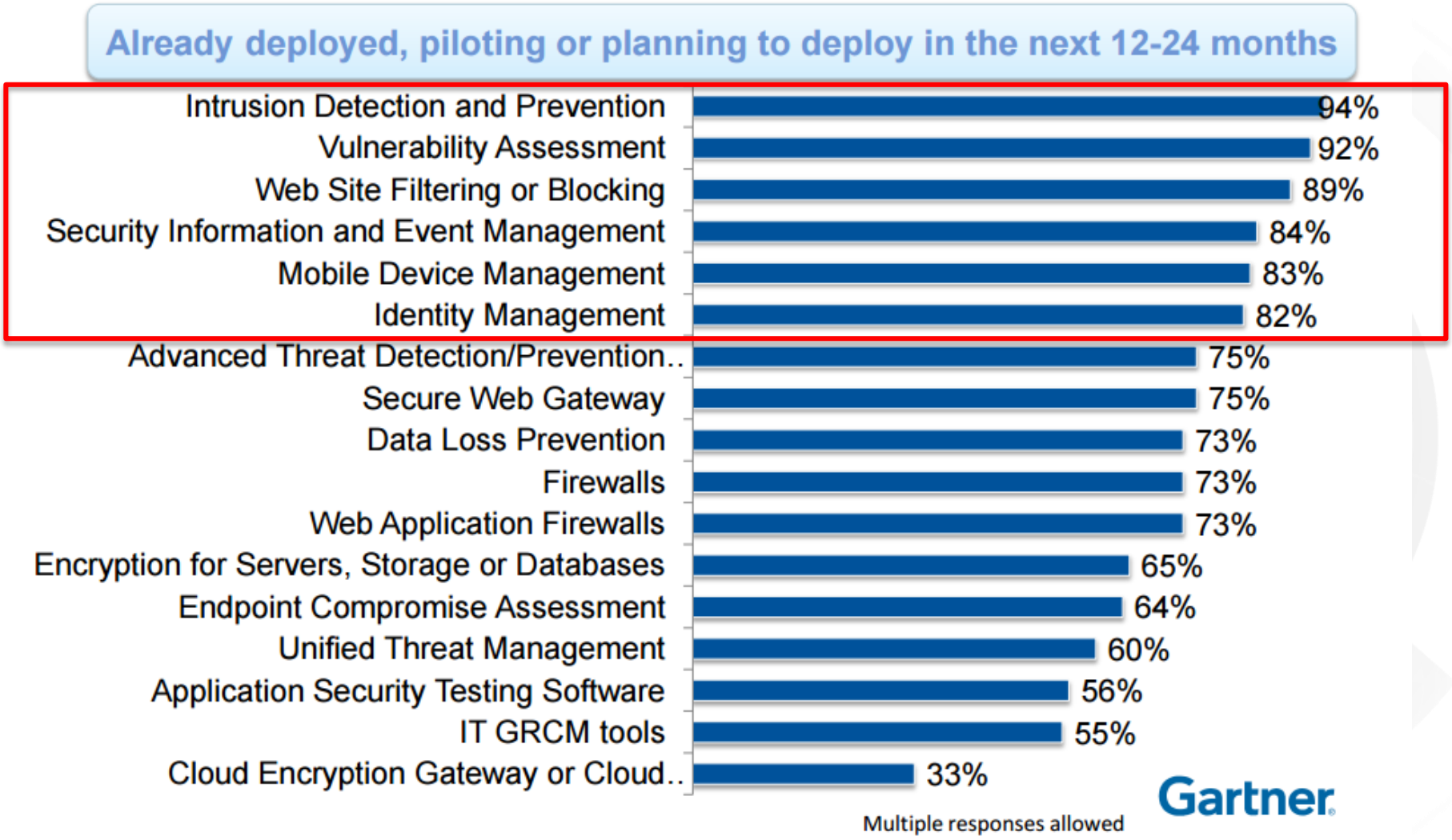
GARTNER



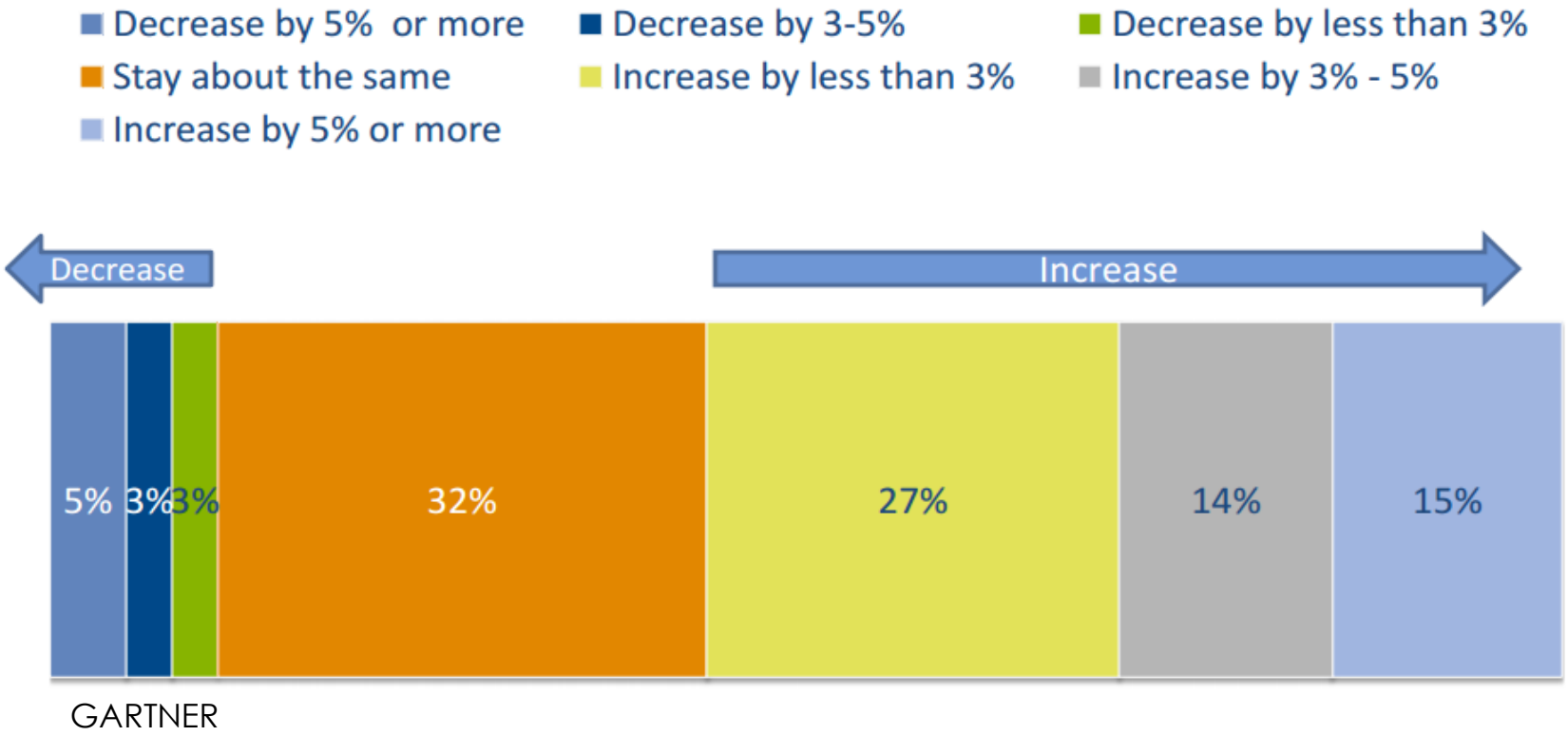
About one in every eight organizations does an extremely poor job of:

- *Risk and controls assessment*
- *Threat and vulnerability management*
- *Event detection and response*
- *Architecture and engineering*

GARTNER


Already deployed, piloting or planning to deploy in the next 12-24 months
Intrusion Detection and Prevention 94%
Vulnerability Assessment 92%
Web Site Filtering or Blocking 89%
Security Information and Event Management 84%
Mobile Device Management 83%
Identity Management 82%
Advanced Threat Detection/Prevention.. 75%
Secure Web Gateway 75%
Data Loss Prevention 73%
Firewalls 73%
Web Application Firewalls 73%
Encryption for Servers, Storage or Databases 65%
Endpoint Compromise Assessment 64%
Unified Threat Management 60%
Application Security Testing Software 56%
IT GRCM tools 55%
Cloud Encryption Gateway or Cloud.. 33%
Gartner
Multiple responses allowed

Anticipated change in IT security budget



GARTNER

IS YOUR WINDOW BROKEN?

SIMPLE INFOSEC SELF ASSESSMENT
(rs@integrity.pt)

SIMPLE INFOSEC SELF ASSESSMENT
Obscurity is not Security

How Often?

Maybe Quarterly..

Source:

- What I Know
- What I Saw
- What I Heard
- What Happened

Keep in mind that - Simple is just the antonym of complex and complicated...

SIMPLE INFOSEC SELF ASSESSMENT
Obscurity is not Security

Cenário:

"Se eu quisesse obter acesso ilegítimo, provocar danos ou um incidente na minha organização:

- Por onde começava? [Enumerate 5]
- Quão fácil seria? [Scale 1-5]
- Quão Provável seria de ter sucesso? [Scale 1-5]
- Quanto custa minimizar ou resolver?" [Scale 1-5]

SIMPLE INFOSEC SELF ASSESSMENT
Obscurity is not Security

Item	Order		Easyness		Probability		Cost to solve	SCORE
Item 1	5	x	3	x	2	÷	2	15
Item 2	4	x	2	x	5	÷	4	10
Item 3	3	x	1	x	3	÷	5	1.8
Item 4	2	x	5	x	2	÷	3	6.66
Item 5	1	x	4	x	1	÷	1	4

IF SCORE > 5 :
Considerar colocar o assunto na agenda pela prioridade do score...

telnet your.mailserver.com:25
helo mailserver.com
mail from: contabilidade@seufornecedor.com
rcpt to: sua_contabilidade@suaempresa.com
data
subject: IMPORTANTE – Alteração de NIB
Exmos Senhores,

Informamos que alterámos o nosso NIB e de acordo com o procedimento instituído informamos que todas as facturas de agora em diante devem ser pagas para o NIB:

BANCO XXXXXXX
NIB: <INSERT 21 DIGITS HERE>

Atentamente,
.

UTILIZADORES

Além End-Point Security
Consciencializar
Suportar os Utilizadores:
OTP / FDE / …

DADOS

Conhecer os Dados
Categorizar Aplicações
Segmentar os Dados
Mascarar e Associar
Conhecer os Padrões de Uso
Gestão Privilégios (Detalhado)
Marcar para Detectar

ANTECIPAR

Simular Situações de Ataque
Formar / Treinar
Incident Response
Situational Awareness
CyberAttack Recovery Plan
Persistent PenTesting
Vulnerability Management

INFRA-ESTRUTURA PLATAFORMAS

Assumir Existência 0-Days
Segmentar
Isolar
Conhecer as Baselines
Incrementar Resiliência

ORGANIZAÇÃO

Gestão de Risco
Definir Responsabilidades
Gerir
Operar
Monitorizar
Gerir 3rd Parties Risk

DETECTAR

Padrões Anormais de Utilização
Monitorizar Integridade / Detectar Alterações
Utilização de dados "marcados"
Monitorização associações
SIEM

INTEGRITY

consulting & advisory

INTEGRITY Portugal
Av. João Crisóstomo, 30 5º
1050-127 | Lisboa - Portugal
info@integrity.pt
+351 21 33 03 740

INTEGRITY United Kingdom
Suite 4B | 43 Berkeley Square
Mayfair, Westminster |
London W1J 5FJ – UK
+44 20 3318 0800

www.integrity.pt
www.keepitsecure24.com