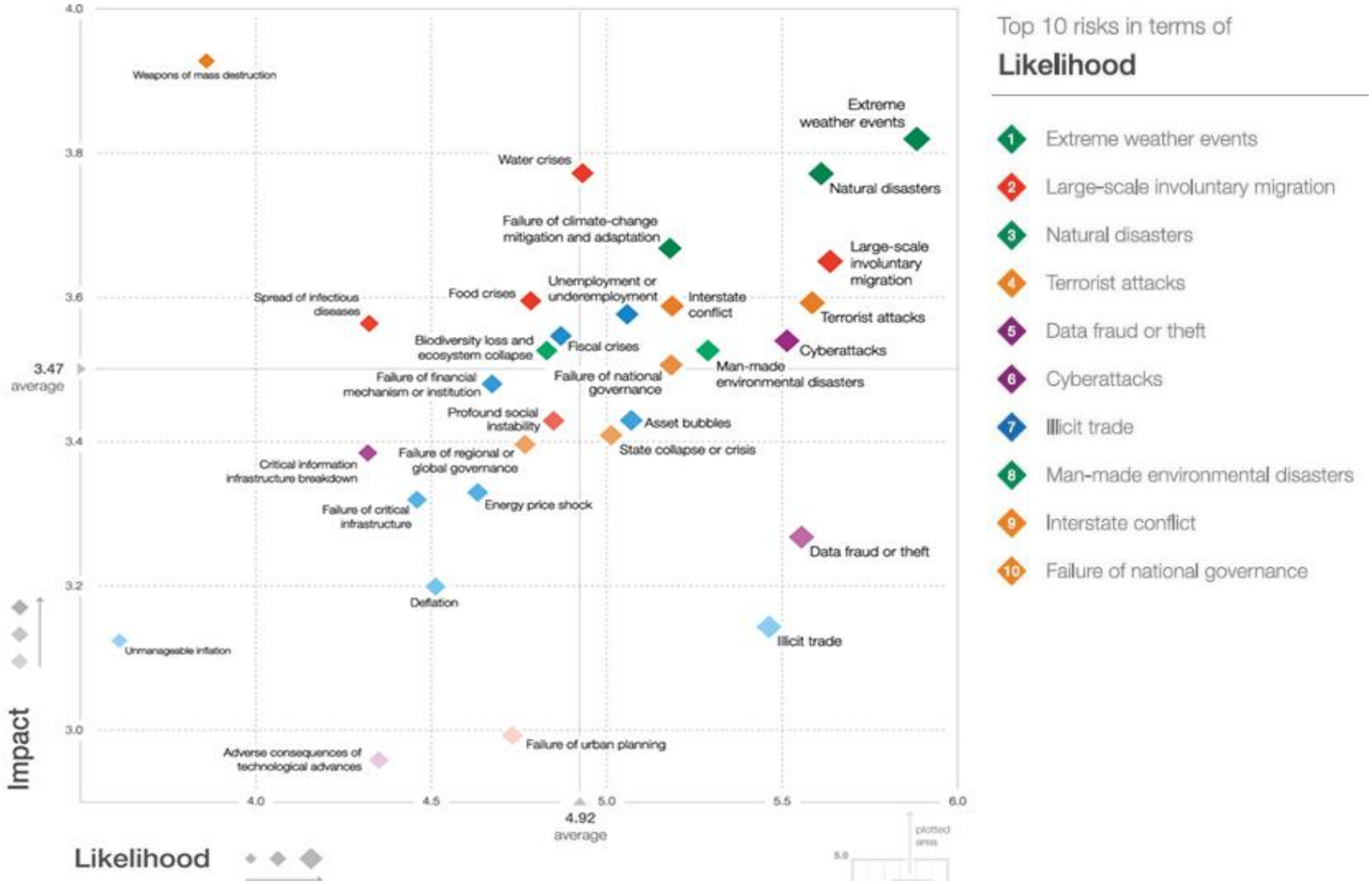
RISCOS CIBERNÉTICOS XVI ENCONTRO SETOR ELÉTRICO

JUNHO 2017

RISCOS CIBERNÉTICOS
COMPARATIVO DAS DEMAIS AMEAÇAS



Fonte: World Economic Forum Report 2017

ALGUNS NÚMEROS
RISCO CIBERNÉTICO

59

INCIDENTES NO SEGMENTO DE ENERGIA EM 2016

reportados ao Homeland Dep. USA

Fonte: Houston chronicle

O VALOR DE RELATÓRIOS CORPORATIVOS

entre $547 e $822

Fonte: Ponemon

RAMSOMWARE

Custo médio por incidente $156,900. Em media 1 empresa é atacada a cada 40”

Fonte: Ponemon

ALGUNS NÚMEROS

RISCO CIBERNÉTICO

61%

C-LEVEL LEADERS

Vêem ameaças cibernéticas como um risco direto aos negócios

Fonte: JLT Decoder

$1.87bi

Devem ser investidos em mitigação de perdas cibernéticas pelo setor de energia até 2018

Fonte: World Energy Ccouncil

1,378,509,261

Em dados comprometidos em 2016

Fonte: Kaspersky

$5,85m

Custos de violação em empresas Americanas de Energia

Fonte: enews

$445bi

Valor de perda estimada para Economia Global

Fonte: McAfee

ATAQUE E DEFESA SEGURO
RISCO CIBERNÉTICO

BRASIL SNAPSHOT

- $$ = U$$ 8 bilhões em perdas financeiras em 2015.
  Fonte: McAfee

- 6,6% de todos os crimes cibernéticos financeiros no mundo ocorreram no Brasil.
  Fonte: CPqD, Centro de Pesquisa e Desenvolvimento em Telecomunicações

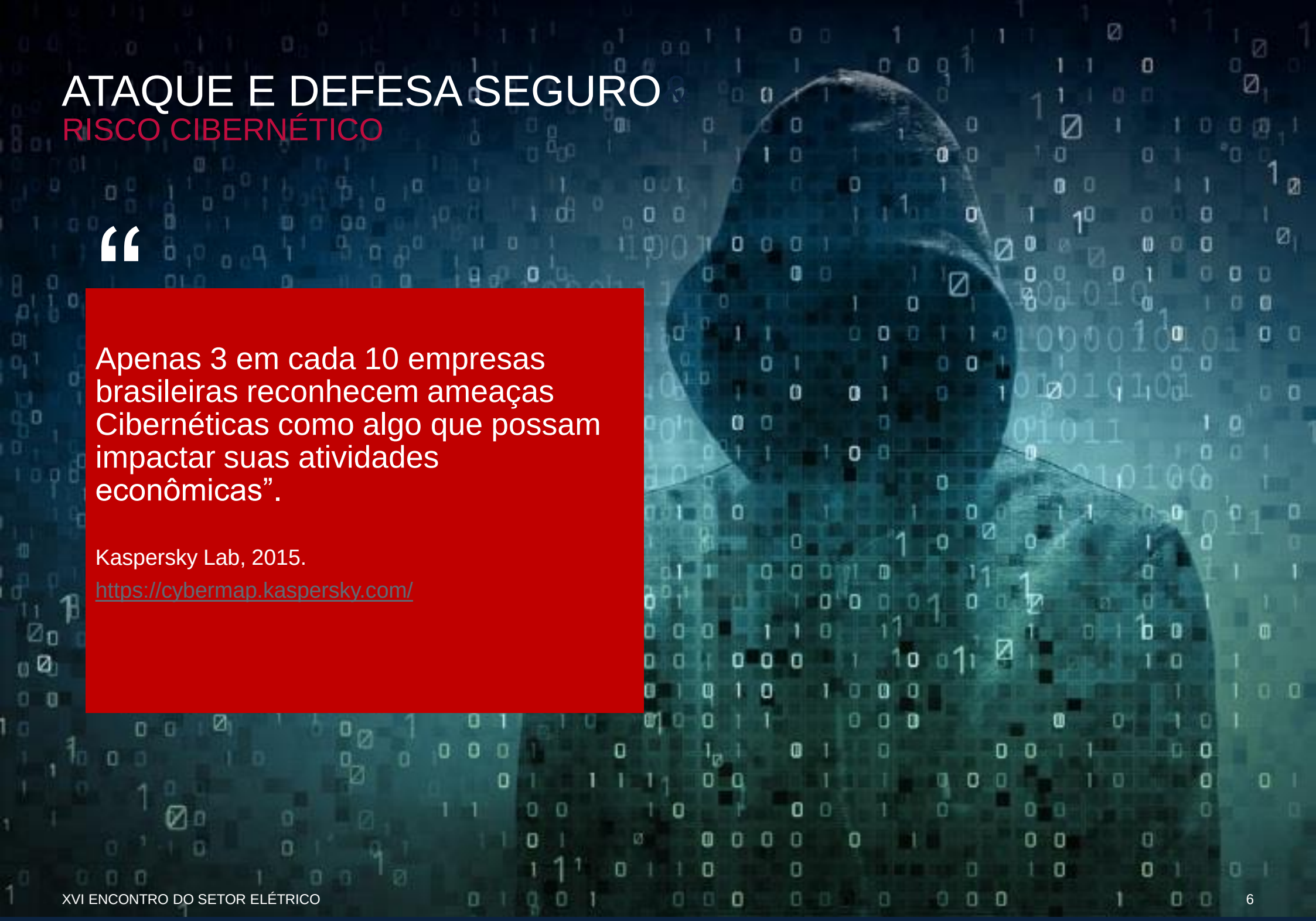
- 8° dentre os países com maior atividade maliciosa no mundo.
  Fonte: Symantec

- 5º país mais afetado no ataque do WannaCry com 2.114 infecções.
  Fonte: Avast

- O ministro da Mineração e Energia reportou tentativas de ataques para roubo de informações classificadas.
  Fonte: Zurich

ATAQUE E DEFESA SEGURO

RISCO CIBERNÉTICO



“

Apenas 3 em cada 10 empresas brasileiras reconhecem ameaças Cibernéticas como algo que possam impactar suas atividades econômicas”.

Kaspersky Lab, 2015.

https://cybermap.kaspersky.com/

CENÁRIO DO BRASIL
RISCO CIBERNÉTICO

CRESCIMENTO DOS INCIDENTES DE CYBER

Brasil	**274%**
Mundo	**38%**

APONTAM PERDAS FINANCEIRAS EM INCIDENTES CYBER

Brasil	**39%**
Mundo	**25%**

RELATAM IMPACTOS RELACIONADOS AOS REGISTROS DE SEUS CLIENTES

Brasil	**46%**
Mundo	**38%**

APONTAM COLABORADORES ATIVOS COMO ORIGEM DOS INCIDENTES DE CYBER

Brasil	**41%**
Mundo	**34%**

Fonte: CPqD, Centro de Pesquisa e Desenvolvimento em Telecomunicações

A CULPA É DO TI
RESPALDO DE LEI:

Lei:

- 2014 – Lei 12.965 Marco Civil da Internet:

Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

a) - **Neutralidade da rede** (art. 9, § 1º);
b) - **Privacidade na rede** (art. 10, § 4º; art. 11, § 3º e art. 11, § 4º);
c) - **Guarda de registros** (art. 13 e art. 15).

Projetos de Lei:

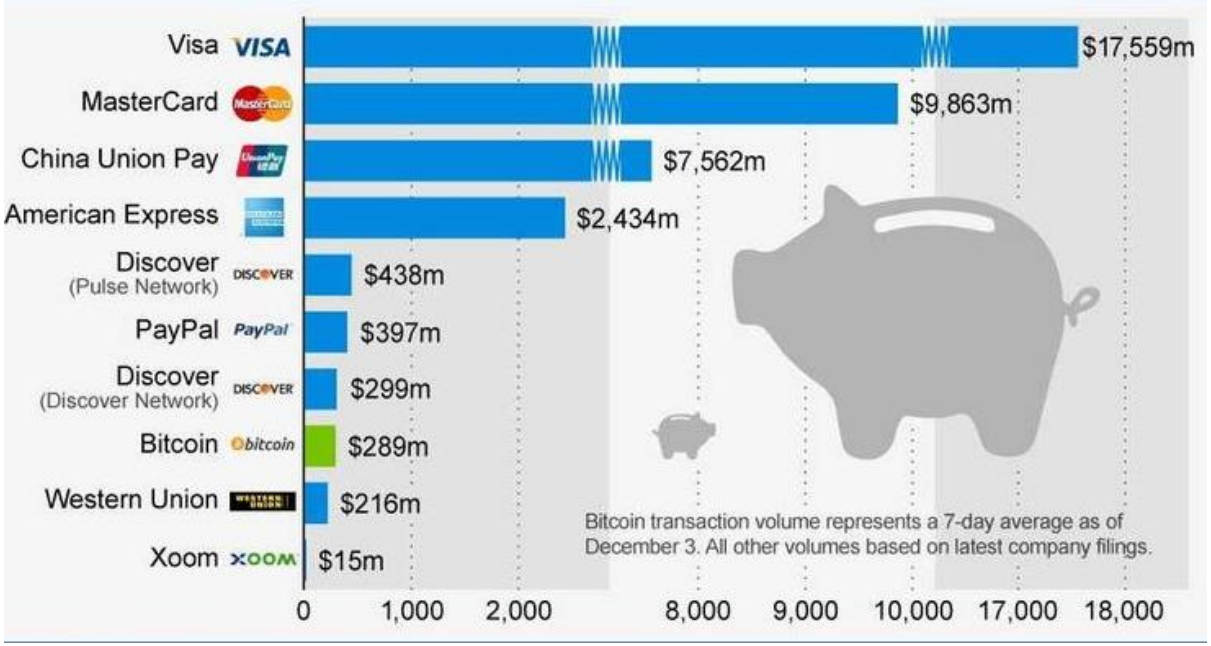
- 2012 – PL 271 Senado – Estabelece Dever de Notificação.

- 2012 – PL 4060 da Câmara – Projeto de Lei de Proteção de Dados.

- 2014 – PL 181 do Senado – Projeto de Lei de Proteção de Dados.

VOLUME DE TRANSAÇÕES DE BITCOIN

comparado a outros métodos de pagamentos



Fonte: COINOMETRICS

Volume médio diário de transações de redes de pagamento selecionadas (em milhões de dólares)

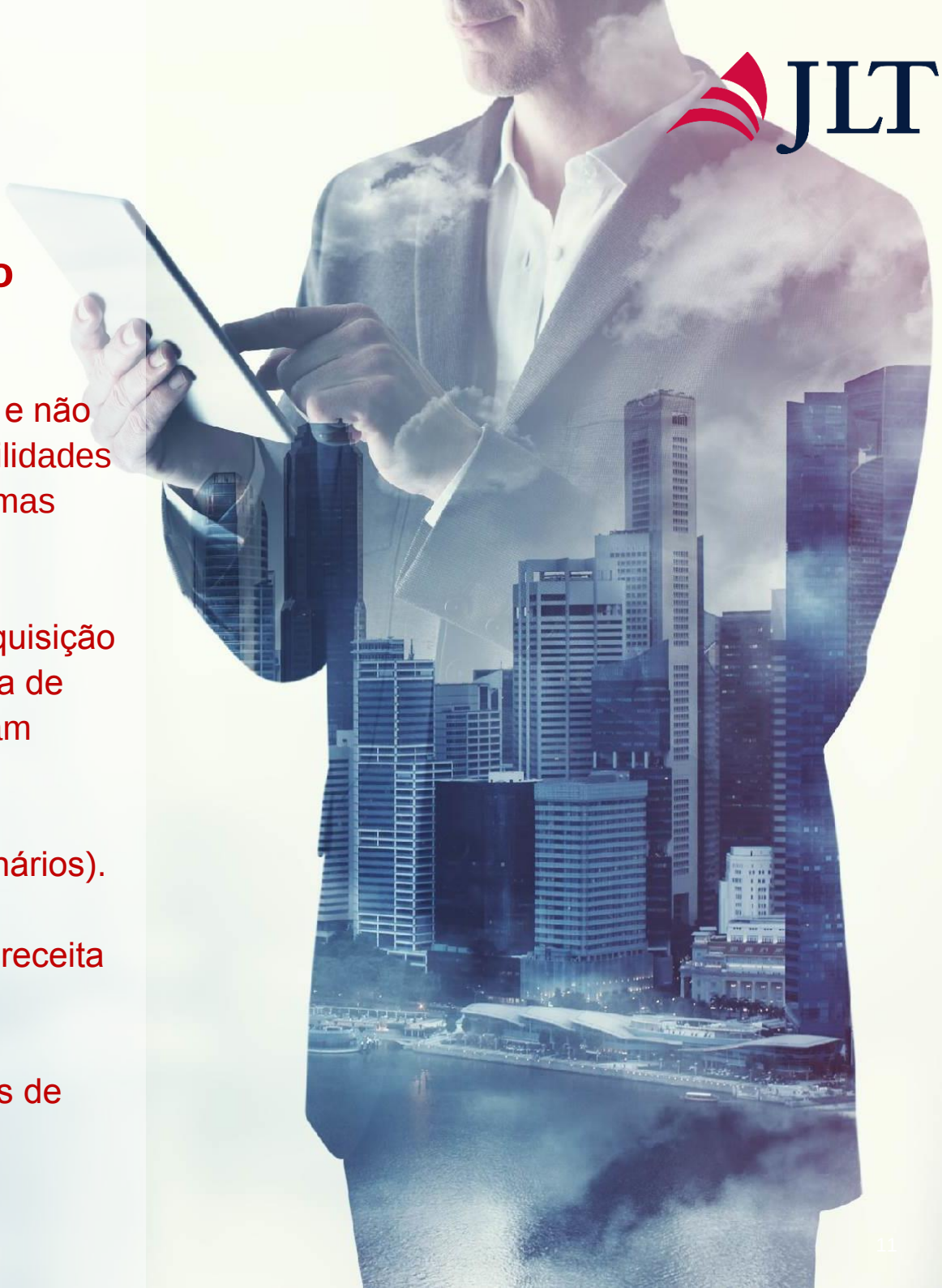
A CULPA É DO TI
RISCO CIBERNÉTICO

O departamento de TI trabalha para reduzir de forma diligente e proativa o risco de uma violação ou ataque com firewalls, software e antivírus, e é importante notar que uma Apólice de Riscos Cibernéticos não está destinada a substituir esta função, mas cobrir os custos incorridos pela violação de dados.

OS TRÊS ELEMENTOS BÁSICOS DA COBERTURA CYBER: PREVENÇÃO, TRANSFERÊNCIA E REAÇÃO

Nós não queremos que o seguro seja um substituto para a segurança!

SETOR ELÉTRICO
RISCOS DO SETOR



Quais são os principais riscos para o setor energia?

• Recursos alocados para segurança física (IOT) e não de informação e sistemas, resultam em vulnerabilidades de segurança devido ao grande número de sistemas conectados à dispositivos simples.

• Sistemas sofisticados de controle industrial e aquisição de dados (SCADA) visados por hackers. "Sistema de Controle de Informação" (ICS) atuais compartilham informações via rede.

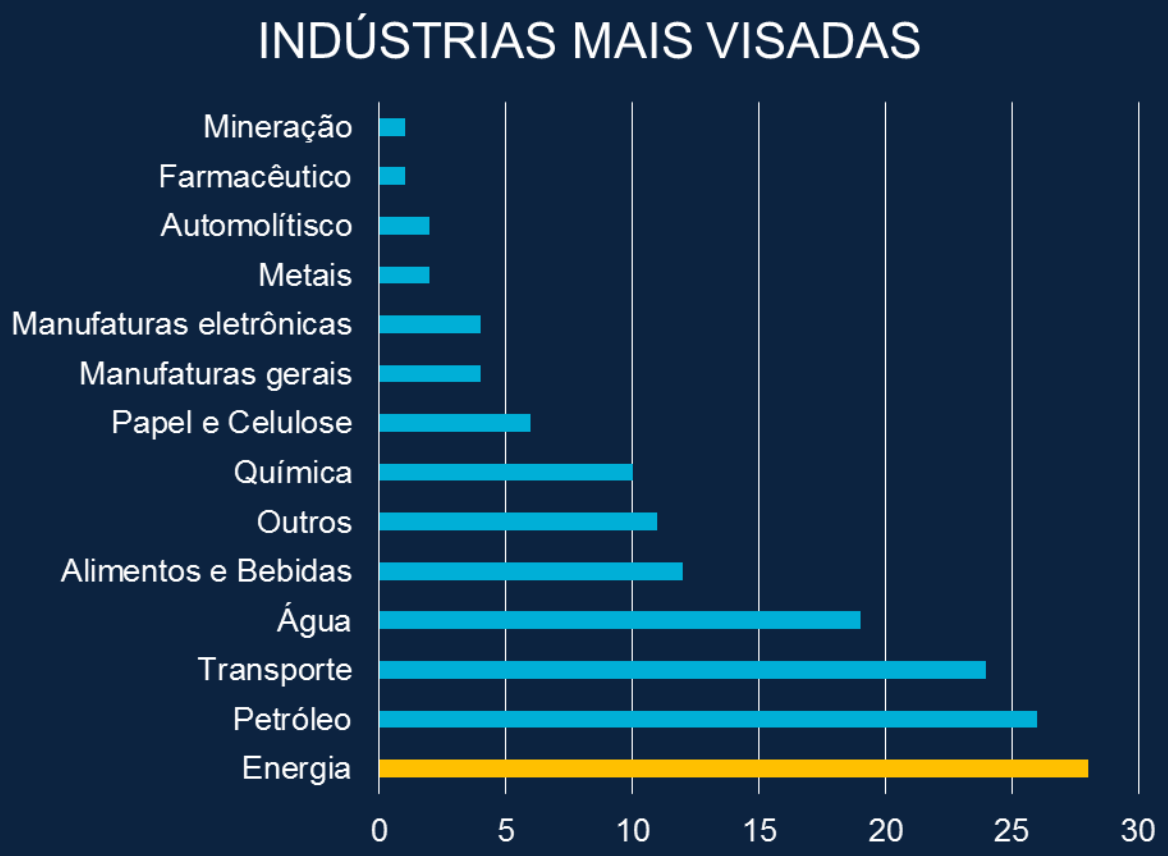
• Perdas de dados de terceiros (clientes e funcionários).

• Interrupção de negócios / serviços ou perda de receita devido a incidente cibernético.

• Lesões corporais ou danos materiais resultantes de incidentes cibernéticos.

SETOR DE ENERGIA
RANKING

"O aumento da interconexão e digitalização do setor de energia e seu papel crítico no funcionamento de uma economia moderna tornam o setor um alvo altamente atraente para ataques cibernéticos destinados a interromper as operações". World Energy Council 2016



Fonte: Repository of Industrial Security Incidents/Security Incidents Org.

INTERNET DAS COISAS (IOT)
SETOR ELÉTRICO

The Industrial Internet is transforming the way people service and maintain industrial equipment, medical devices and other machines.

Intelligent Machines

Through self-monitoring and transmission of sensor data, intelligent machines enable preventative maintenance and move closer to the goal of "no unplanned downtime."

Transmitting Valuable Data

Real-time information on the condition of individual assets reduces the need for higher-cost scheduled maintenance.

Optimizing Operations

Operations centers engage in data segmentation and filtering for customized "fleet" views, historical analysis, real-time analysis and forecasting.

Empowering Technicians

The Industrial Internet provides workers with information and resources in real-time, improving productivity and driving more efficient work practices.

ATIVOS EMPRESARIAIS
RISCO ASSEGURÁVEIS

As empresas compram seguro para proteger seus ativos no entanto apenas contabilizando 30% dos ativos os quais são tangíveis, mas deixam 70% que são intangíveis em risco. (Ernst & Young)

Tradicionais

- PRÉDIO
- FROTA
- RESPONSABILIDADE CIVIL
- EMPREGADOS (BENEFÍCIOS, D&O)
- MERCADORIAS E MATÉRIA PRIMA
- RESPONSABILIDADE CIVIL

Digitais

- INFORMAÇÕES CONFIDENCIAIS
- SOFTWARE E SISTEMAS
- REPUTAÇÃO
- WEBSITE E MÍDIAS SOCIAIS
- PRODUTOS E ESTRATÉGIAS
- TECNOLOGIA

ATAQUE E DEFESA

RISCO CIBERNÉTICO

O Seguro Cyber é um mecanismo para ajudar a compensar os potenciais impactos financeiros de um ataque cibernético.

O QUE PODE CAUSAR	EVENTO	NATUREZA DO EVENTO	IMPACTO DIRETO	CONSEQUÊNCIAS | CUSTOS | SEGURO
• Empregados • Terceiros (fornecedores, clientes) • Hackers	• Extorsão cibernética • Roubo de identidade • Acessos não autorizados • Perda destruição de data • Espionagem • Sequestro de dados • Fraude /crime • Violação de privacidade • Roubo de propriedade intelectual • Roubo de informações privilegiadas • Desconhecido	• Hacking • Virus • Malware • Social engineering • Erros sistêmicos	• Interrupção sistêmicas • Danos a ativos Digitais • Ameaças/ extorsão • Perda de Dados • Interrupção de prestação de serviços	• Perda de receita • Custos com restauração ou reconstrução de dados • Custos de consultoria de Investigação forense • Custos de reparo de imagem – perda de confiança do cliente • Custos jurídicos em relação a responsabilidade civil de dados/serviços de clientes • Custos de notificação • Perda de um ativo (roubo de propriedade intelectual) • Custos adicionais de homem hora para restabelecer serviços

TIMELINE DE RESPOSTA
RISCO CIBERNÉTICO

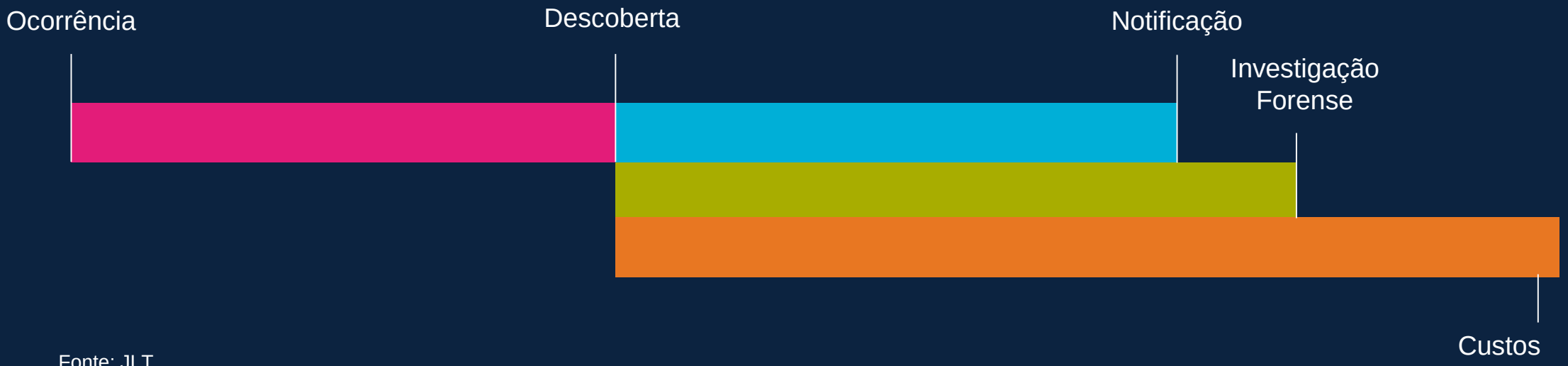
180
Dias
Entre o evento e Descoberta

7
Dias
Entre Descoberta e contenção

43
Dias
Em média de investigações forense

40
Dias
Entre Descoberta e notificações

CUSTOS



Fonte: JLT

CASOS GLOBAIS
SETOR ELÉTRICO

USA/CANADA 2013-2015 GERAÇÃO DE ENERGIA
Erro humano/hacking

Ataque a uma empresa que opera mais de 50 usinas de energia nos EUA e Canadá. Onde foram roubadas informações de projetos críticos de plantas de energia e senhas do sistema.

Korea do Sul | Planta Nuclear
Hacking

Korea Hydro e Nuclear Power Co. sofreu uma série de ataques com a intenção de causar danos aos reatores. Além de algumas más funções de sistemas, os ataques causaram o vazamento de informações confidenciais.

USA 2003 | USINA NUCLEAR
Malware

'Afetados pelo vírus Slammer' que foi de grande impacto em 2003, a qual atacou a rede privada em uma energia nuclear em seus sistema por 5 horas. Cinco outras plantas foram afetadas.

SAUDI ARÁBIA 2012 | OIL & GAS
Virus

O vírus Shamoon infectou 30.000 computadores pertencentes à Saudi Aramco, o maior produtor mundial de petróleo e gás. Alguns sistemas ficaram inoperantes por 10 dias e 85% do harware da empresa foi destruído tendo efeitos recorrentes em toda a economia.

AUSTRÁLIA, 2015 SETOR PÚBLICO
Hacking/virus

Hackers atacaram o Departamento de Recursos e Energia em New Wales. O interesse dos hackers no departamento foi em obter informações de projetos atuais e informações mais altamente classificadas do governo.

CASOS GLOBAIS
SETOR ELÉTRICO

USA, 2013
BARRAGEM
Malware
A pequena barragem de Bowman Avenue, próximo a NYC, é usada para o controle de inundações. Os Hackers obtiveram acesso parcial aos sistemas da barragem usando malware padrão, destacando a vulnerabilidade de toda a infra-estrutura.

Ucrânia 2015
MALHA ENERGÉTICA/ GRID
Hacking/erro humano
Este hack foi bem planejado em 3 powerdistribution causando interrupções de serviços a 80.000 clientes de energia. É o primeiro Hack conhecido para causar uma queda de energia direta. A entrada foi através de um phishing destinada a equipe de TI.

USA, 2013
GERAÇÃO DE ENERGIA
Erro humano/vírus
O ICS de uma empresa de energia dos EUA foi infectado com o Vírus Mariposa quando um técnico de uma empresa terceira contratada para atualizar os sistemas utilizou um USB. O vírus resultou em tempo de inatividade dos sistemas e instalações de aproximadamente 3 semanas.

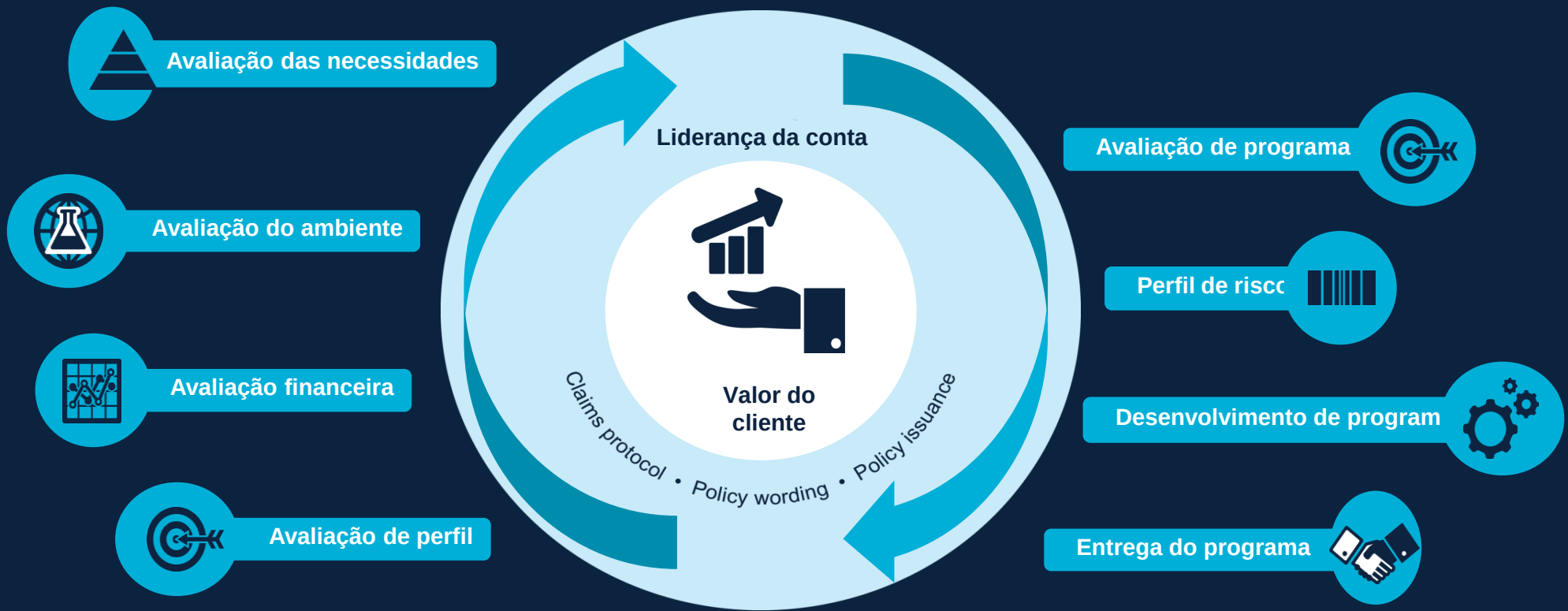
Israel 2016
MALHA ENERGÉTICA
Malware/erro humano
Um funcionário da Autoridade de Eletricidade foi vitima de um ataque de phishing, que infectou um número de computadores na rede. O Grid não foi afetado no entanto afetou parcialmente os serviços e demorou dois dias para a retomada das operações a níveis normais.

O QUE NÓS PODEMOS FAZER POR VOCÊ?

A colocação efetiva de um seguro cibernético depende de uma compreensão das exposições Cyber de organizações.

O QUE NÓS PODEMOS FAZER POR VOCÊ?

RISCO CIBERNÉTICO



PERGUNTAS?

CONTATOS

Lygia Muriel
E: lygia_muriel@jltbrasil.com
T: +55 11 3156-3975

Marta Schuh
E: marta_schuh@jltbrasil.com
T: +55 11 3156-3341