Kroll | A Division of DUFF & PHELPS

Segurança Cibernética e Inovação

Café com Seguro

Novembro de 2019

Agenda

Sobre o palestrante e a Kroll

O momento da Segurança Cibernética

Inovação? Seguro Cibernético

Dúvidas e questionamentos

1.

Sobre o palestrante e a Kroll

Walmir Freitas

Sr. Vice President
Cyber Security

Av. Jornalista Roberto Marinho 85, 5.º andar
Vila Olímpia São Paulo 04547-005 Brasil

walmir.freitas@kroll.com
+55 11 3897 0916

Walmir Freitas é Sr. Vice President e líder da prática de Cyber da KROLL no Brasil.

Com mais de 21 anos de experiência em Segurança da Informação e Cibernética, Walmir liderou diversos projetos de grande complexidade, tendo uma carreira focada em consultoria passando pelas especializações de Gestão de Privacidade e Conformidade com LGPD e GDPR, Resiliência Cibernética, Cyber Intelligence e Prevenção à Fraudes Digitais.

Entre suas principais conquistas, Walmir como CISO de um processadora de pagamentos conduziu os processos de adequação ao PCI DSS sendo essa empresa a primeira emissora certificada no Brasil. Adicionalmente, trabalhou junto a bureaus de crédito no estabelecimento da abordagem de segurança necessária para o estabelecimento do Cadastro Positivo no Brasil.

Previamente à sua entrada na Kroll, liderou áreas de segurança e competência em empresas como IBM, Accenture, Deloitte e EY, possuindo as certificações mais relevantes no mercado (CISSP, CISM, CISA, CGEIT, CRISC e CBCP).

Sobre a KROLL | DUFF & PHELPS

A Duff & Phelps é um consultoria global que protege, restaura e maximiza o valor para seus clientes nas áreas de avaliação, finanças corporativas, investigações, disputas, segurança cibernética, conformidade e assuntos regulatórios, além de outros aspectos relacionadas à governança. Trabalhamos com clientes em diversos setores, mitigando riscos para ativos, operações e pessoas.

MAIS DE 15.000 PROJETOS EXECUTADOS EM 2017

6.500 CLIENTES INCLUINDO MAIS DE **50%** OF THE **S&P 500**

Mais de 70 escritórios em 28 países

Kroll | Duff & Phelps TRABALHA COM MAIS DE **70%** DOS CLIENTES DA *FORTUNE* **100**

AS AMÉRICAS CONTAM COM **2.000+** PROFISSIONAIS

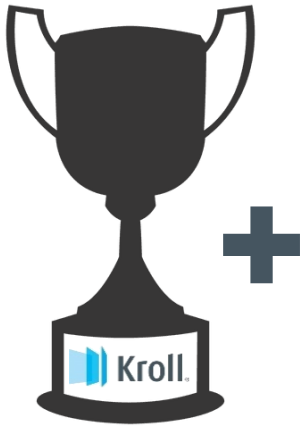
EUROPA E ORIENTE MÉDIO CONTAM COM **1000+** PROFISSIONAIS

ÁSIA PACIFICO **500+** PROFISSIONAIS

Os especialistas da Kroll possuem **mais 30 tipos de certificações da indústria**, incluindo CIPP/US,CRISC, CISA, CISM, CISSP, CPP, GCIH, GREM, GNFA, GPEN, MCP, MCSE, PFI, PMP, QSA,CEH.

Sobre a KROLL | DUFF & PHELPS

THE NATIONAL LAW JOURNAL FORRESTER



E seu time

Reconhecimento global

Líder global em *cyber security*, *compliance*, e investigações

Uma oferta completa e multidisciplinar de serviços e soluções integradas.

Certificações e prêmios que demonstram a **qualidade de nossos serviços.**

Expertise na condução de situações emergenciais

Senioridade profissional

Profissionais com mais de **20 anos de experiência** no mercado cibernético.

Profissionais certificados em framework reconhecidos como por exemplo: **PCI QSA e ISO 27001.**

Experiência comprovada

Exemplos de clientes em projetos similares

CIELO	XP	Banco Pan
AIG	WEX INC	HARMONIA
ZAPAY	ITAÚ	MACHADO MEYER
SERASA	PAGOLIVRE	SODEXO

Reconhecimento da indústria

THE NATIONAL LAW JOURNAL BEST OF 2018 WINNER
- Best Cyber Security Provider
- Best Litigation Dispute Advisory Services Consultant
- Best Corporate Investigations Provider
- Best Data Security Provider
- Best Managed IT Service Provider
- Best Global Risk & Investigations Consultant

> *[Kroll] is capable of being a one-stop shop for multiple services relating to breach response, from forensic investigations to support for clients in litigation issues.*

FORRESTER® WAVE LEADER 2017
Customer Data Breach Notification And Response Services

THE NATIONAL LAW JOURNAL BEST OF 2018 HALL OF FAME
KROLL

CORPORATE COUNSEL AWARDS
- Cyber Security Provider
- Managed IT Services Provider
- Corporate Investigations Provider
- Litigation Dispute Advisory Services Consultant
- Global Risk & Investigations Consultant

Produtos e Serviços

Proteger

- **Cyber Risk Assessments (HIPAA, NY-DFS, GDPR, etc.)**
- **Cyber Policy Review & Design**
- **Interim CISO & Data Protection Officer for GDPR and LGPD**
- **Cyber Security & Privacy Considerations for GDPR/LGPD**
- Incident Response Plan and Tabletop Exercises
- Penetration Testing
- Vulnerability Scanning
- Third Party Cyber Audits and Reviews
- QSA/PCI Services
- **Third Party Cyber Risk Rating (CyberClarity360)**

Detectar

- Malware and Advanced Persistent Threat Detection
- Deep and Dark Web Threat Monitoring
- Social Media Threat Monitoring
- Endpoint Detection and Response
- Business Email Compromise Investigations

Responder

- Digital Forensics
- Incident Response Management
- Data Collection & Preservation
- **PCI Forensic Investigator (PFI)**
- Data Recovery & Forensic Analysis
- **Office365 Witness Tool**
- Cyber Litigation Support
- B2B Breach Response
  - Notification Letters
  - Call Center Services

Restaurar

- Credit Monitoring (Kroll Branded)
- Identity Theft Restoration (Kroll Branded)
- Identity Monitoring (Kroll Branded)
- B2B2C: Consumer ID Theft Protection Services

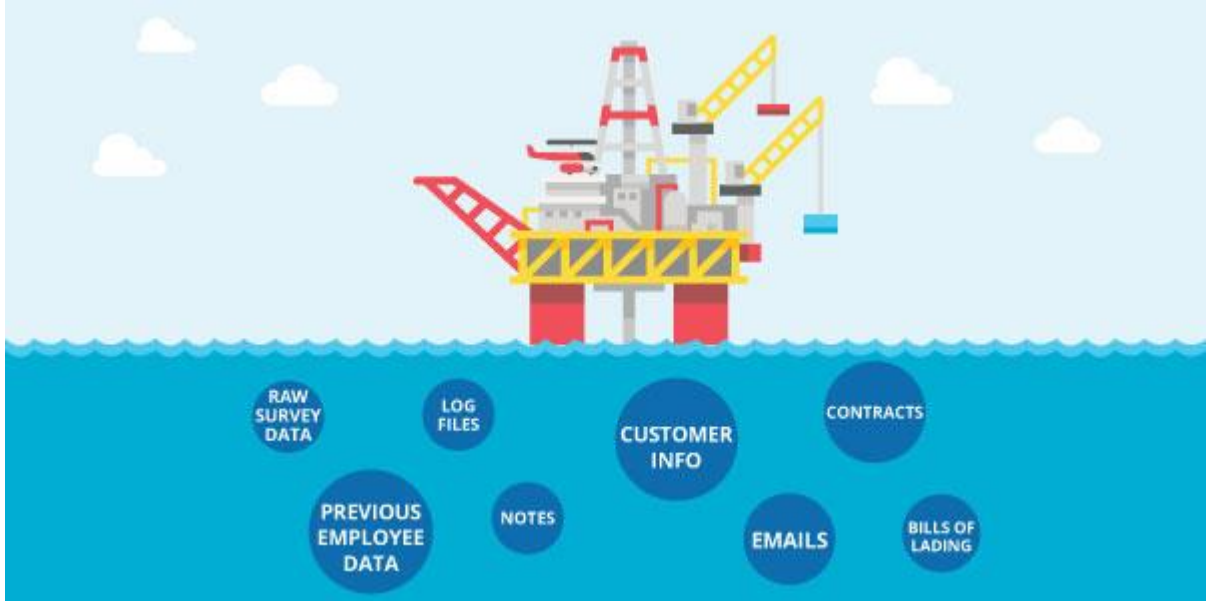
2.

O Momento da Segurança Cibernética

Os dados são o novo “petróleo”?

“Data is the new oil. It’s valuable, but if unrefined it cannot really be used (…) so must data be broken down, analyzed for it to have value.”

Clive Humby, Matemático Inglês.



Será que essa afirmação é válida em todos os contextos?

LGPD – Frenesi ou mudança de paradigmas?

A LGPD prevê a proteção dos dados pessoais seguindo as boas práticas de mercado, além disso, requer um tratamento diferenciado para os dados sensíveis, se vinculados ao indivíduo.

Dados pessoais

- NOME COMPLETO
- NOME DOS PAIS E CONJUGE
- ENDEREÇO
- RG, CPF e CNH
- PASSAPORTE
- SALÁRIO/RENDA
- TELEFONES
- DESPESAS E RECEITAS
- DATA DE NASCIMENTO
- SEXO
- ESTADO CIVÍL
- CERTIFICADOS E NUMEROS DE LICENÇA
- ENDEREÇO DE E-MAIL
- CONTAS BANCÁRIAS
- CARTÕES DE PAGAMENTOS
- DADOS DAS TRANSAÇÃO/OPERAÇÃO

Dados pessoais sensíveis

- IDENTIFICADOR BIOMÉTRICO / GENÉTICO
- IMAGEM, VIDEO E VOZ IDENTIFICÁVEL
- PHI (INFORMAÇÕES MÉDICAS OU DE SAÚDE)
- OPINIÃO POLÍTICA
- OPINIÃO RELIGIOSA
- ORIENTAÇÃO SEXUAL
- ANTECEDENTE CRIMINAL
- GEOLOCALIZAÇÃO
- COOKIES (testemunhos de conexão)
- FILIAÇÃO A SINDICADO

Conceito da Lei:

O dado pessoal é a Informação relacionada a pessoa natural identificada ou identificável.

O dado pessoal sensível é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Sobre a Lei

Necessidade de coletar apenas os dados utilizados

Finalidade no uso do dado e **adequação** compatível

Livre acesso aos seus dados

Manter a **qualidade dos dados**

Principais objetivos da LGPD

Equalizar os direitos entre titular dos dados e as organizações

Minimizar a ocorrência de incidentes de vazamentos dos dados

Risk

Agosto 2020

Manter níveis adequados de **prevenção** e **segurança**

Não utilizar dados para **discriminação**

Demonstrar **responsabilidade** e **prestação de contas** com as normas

Impactos reais

Impacto financeiro, incluindo queda dos valores de mercado

stone

DIVULGAÇÃO DO VAZAMENTO — 24/10/18

IPO — 25/10/18

- Divulgação de **vazamento** de informações **1 dia** antes da abertura de IPO.
- Queda de **8%** no valor das ações, após **1 semana** da abertura de capital.
- Dados vazados: **Código fonte** de uma aplicação de pagamento.
- Vazamento originado por **Colaborador Interno.**

inter

IPO — 01/05/18

DIVULGAÇÃO DO VAZAMENTO — 16/08/18

- Após 3 dias da abertura do IPO, iniciou-se a chantagem para divulgação de dados.
- Queda de **6%** no valor das ações, após 1 dia da divulgação do vazamento de dados.
- Dados vazados: 40GB de **dados de clientes.**
- Vazamento originado por **Terceiro** com acesso a base de dados interna.
- **1,5 MM** em multas (MPF).

NETSHOES

IPO — 12/04/17

DIVULGAÇÃO DO VAZAMENTO — FINAL DE 2017

- Divulgação do vazamento ocorreu entre o fim de 2017 e início de 2018.
- Um dos fatores de influência na tendência de **queda nas ações.**
- Dados vazados: **2,5 MM** de dados de clientes.
- Vazamento originado por **ataque Hacker.**
- **500 Mil** em multas (MPF).

EQUIFAX — 2017

145 milhões de impactados

$1.4 bilhões Moody's Investors Service

de gastos estimados até 2020

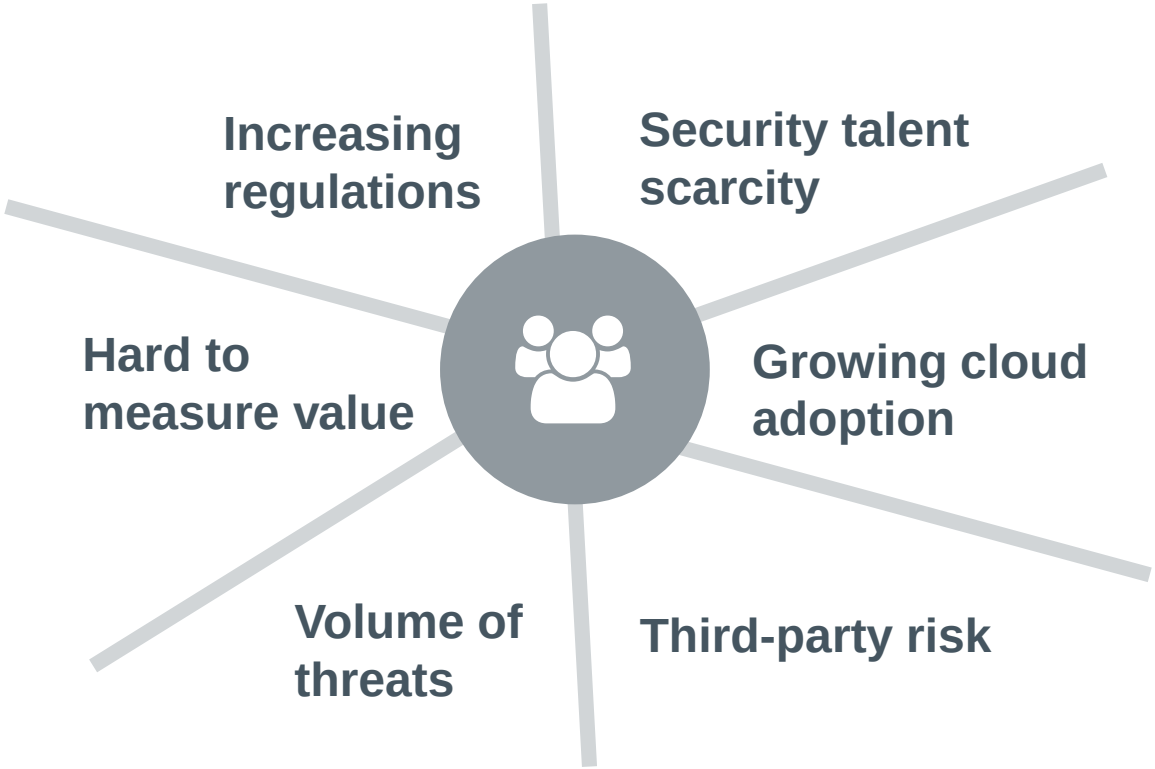
Marriott / Starwood Hotels and Resorts — 2019

382 milhões de impactados

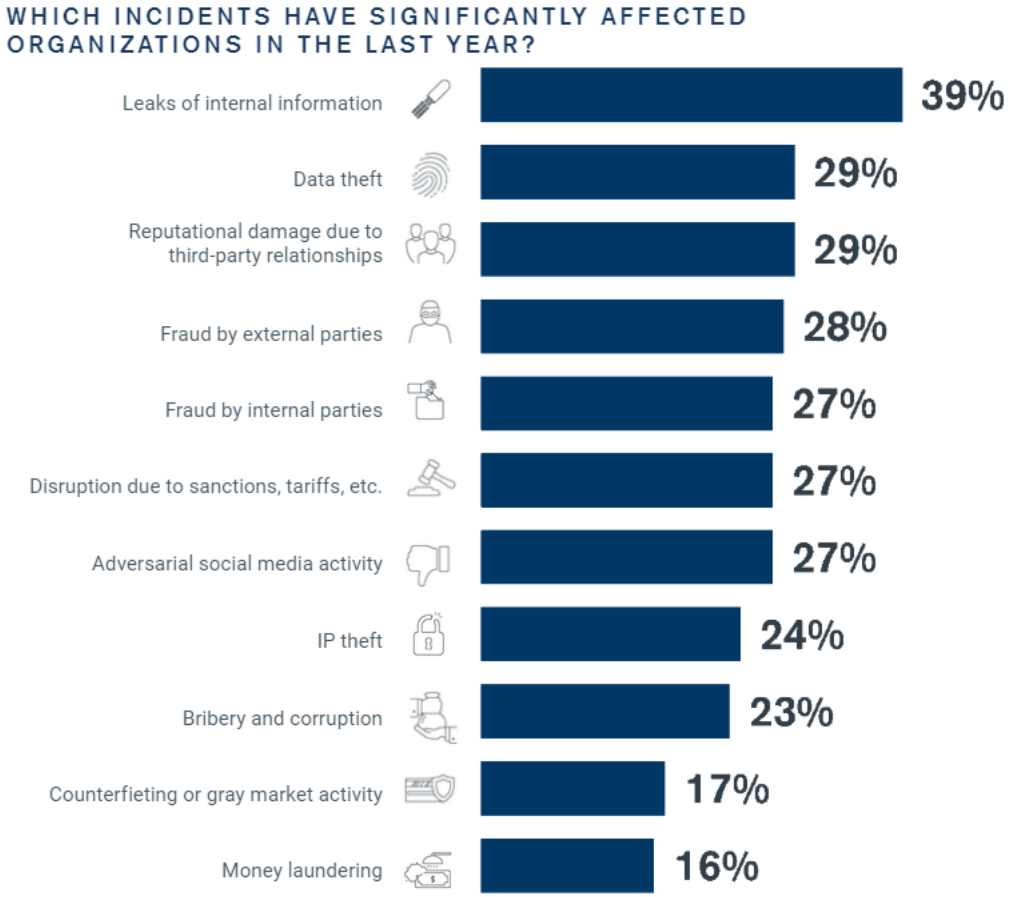
$124 milhões

de multa por descumprir GDPR (UK)

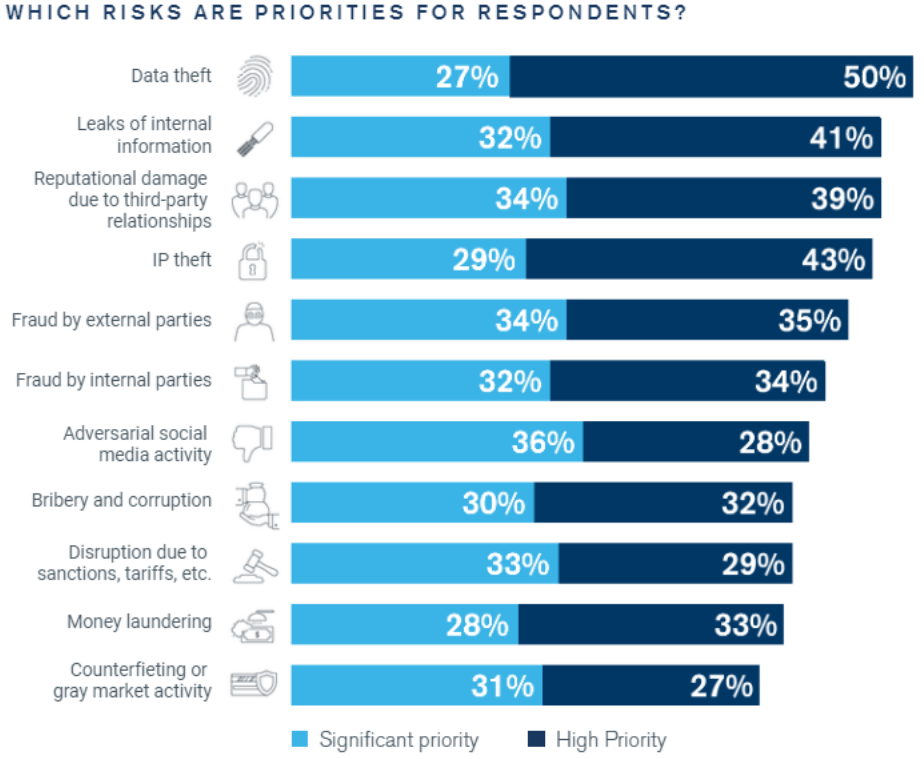
Quais as preocupações dos Executivos?



Quais as preocupações dos Executivos?



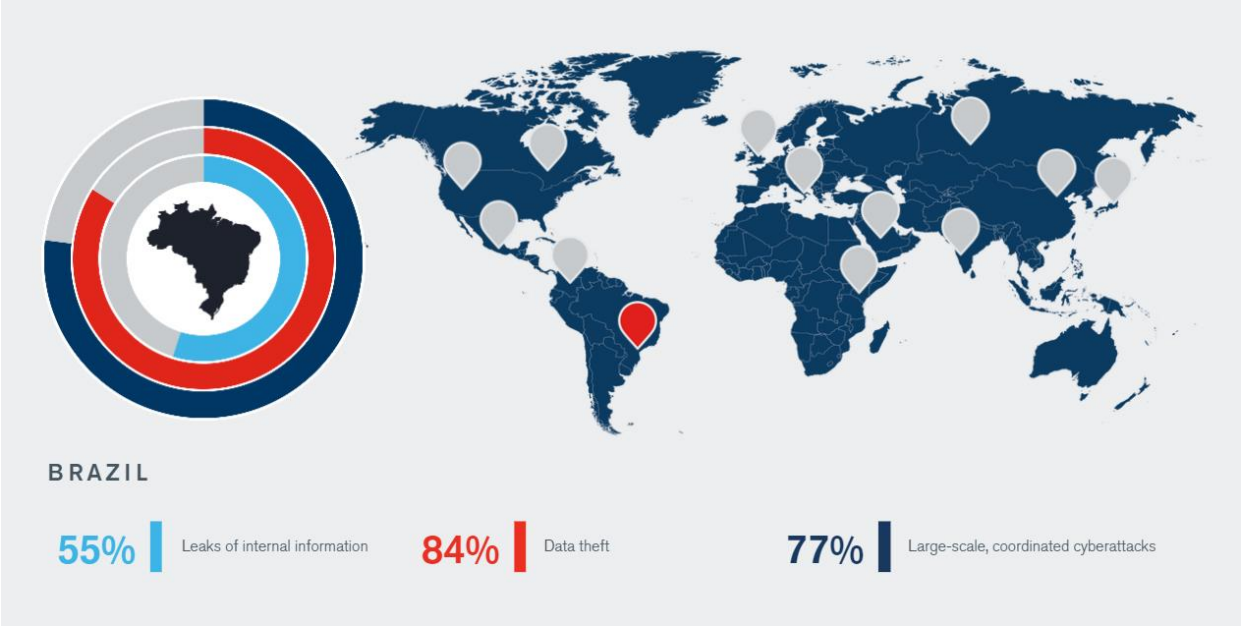
Source: 2019 Forrester Consulting survey commissioned by Kroll of 588 global senior executives



Source: 2019 Forrester Consulting survey commissioned by Kroll of 588 global senior executives

Quais as preocupações dos Executivos?

- Empresários brasileiros consideram o roubo de dados o principal risco para as organizações. A preocupação no Brasil está 8% acima da média global (84% vs 76%). Para enfrentar os ataques, as empresas investem-constantemente em tempo e tecnologia, já que a indústria enfrenta uma corrida cada vez mais acirrada com os criminosos.
- Apesar dos esforços para conter ataques cibernéticos, o maior risco está no vazamento de informações internas. O relatório aponta que o incidente é 16% maior no Brasil do que no restante do mundo (55% vs 39%).
- Além dos investimentos em alta tecnologia, as empresas precisam cuidar de seu ambiente, já que muitas fraudes acontecem por falha humana.



Como nos defender?

Governança	Políticas e Procedimentos	Infraestrutura e Padrões	Pessoas e Treinamentos	Relacionamentos

Frases de efeito porém verdadeiras

- Não existe “bala de prata”
- Tecnologia é apenas 20% da solução

3.

Inovação? Seguro Cibernético

A “Inovação” do Seguro Cibernético

O seguro cibernético é uma solução orientada pelo mercado para melhorar a resiliência do setor privado contra ataques cibernéticos. A cobertura varia de política para política, mas geralmente trata de taxas e despesas legais, bem como os custos associados à notificação de clientes afetados por uma violação, recuperação de dados comprometidos (se possível), reparo de sistemas danificados e compensação pela perda de receita.

1ª Linha de Defesa – Controles de Gestão

- ✓ Abrange o departamento de segurança da informação, bem como várias unidades de negócios que possuem seus riscos cibernéticos. Essas entidades precisam entender como seus ativos são vulneráveis e gerenciar ativamente seus riscos cibernéticos dentro de tolerâncias organizacionalmente aceitáveis

2ª Linha de Defesa – Gestão de Riscos

- ✓ A segunda linha analisa estruturas de controle de segurança cibernética, define KRIs e métricas, cria avaliações de risco e testa e analisa a conformidade rastreando as ações da primeira linha de defesa e analisando o impacto dessas ações para determinar sua eficácia na mitigação de riscos cibernéticos.

3ª Linha de Defesa – Auditoria

- ✓ Assim como na segunda linha de defesa, a terceira linha pode retroceder nas afirmações das linhas anteriores em relação à adequação dos controles em vigor. Essa função geralmente se reporta diretamente ao conselho ou ao comitê de auditoria.

4ª Linha de Defesa
Seguro Cibernético??

A “Inovação” do Seguro Cibernético

Os problemas podem variar porém os mais comuns sao aqueles que se relacionam a interrupção de operações e que podem comprometer a reputação dos clientes.

Ameças mais comuns tratadas pela nossa equipe de Respostas a Incidentes (> 2000 em 2019)	
Business Email Compromise and Wire Fraud	Insider Threats and Accidental Data Loss
Advanced Persistent Threats (APT)	Third Party and Vendor-Related Risks
Malware, Keyloggers, and Backdoors	Cryptocurrency Theft
Ransomware	Targeted Intellectual Property Theft
Payment Card Fraud (PCI/PFI)	Web Application Attacks and Password Theft

A “Inovação” do Seguro Cibernético

Além do acionamento da apólice, as seguradoras tem investido na preparação prévia de seus clientes e também em iniciativas que mitigarão os efeitos de um ataque:

Pró-ativos	Durante o evento
Desenvolvimento de programas de segurança cibernética, serviços virtuais de CISO	Identificação, análise e contenção de ameaças
Análises de Vulnerabilidade/Testes de invasão	**Coordenação com liderança jurídica, de conformidade e de negócios**
Resposta personalizada a incidentes e testes de mesa de notificação	Relatórios personalizados
Workshops de cultura e treinamento em segurança	Suporte a litígios e gestão de evidências
Gerenciamento de Riscos de Terceiros	**Notificações à população impactada**
Dark web monitoring	Melhoria do programa de segurança

A “Inovação” do Seguro Cibernético

Abaixo um caso real de uma **operadora de saúde**, cliente de seguradora, que foi atendida pela Kroll durante um incidente.

Detection

- Time disponível em 2hs após o incidente.
- Time na localidade do cliente identiicando os sistemas comprometidos em 24 hs.

Response

- Por meio de uma soluçao de segurança, a origem do ataque foi eliminada e a contenção estabelecida
- Análise de comprometimento para avaliar a população impactada

Notification

- Estimativas iniciais de 4M + impactadas reduzidas para 2,4M
- População inteira notificada dentro de três dias, por meio de call centers bilíngues

Remediation

- Roubo de identidade + monitoramento de crédito
- Avaliação da exposição na na Dark Web para riscos potenciais

Hardening

- Proteção do Office 365
- Teste de penetração

4.

Dúvidas e questionamentos

Kroll | A Division of DUFF & PHELPS

For more information about our global locations and services, please visit:
www.kroll.com

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, investigations, disputes, cyber security, compliance and regulatory matters, and other governance-related issues. We work with clients across diverse sectors, mitigating risk to assets, operations and people. With Kroll, a division of Duff & Phelps since 2018, our firm has nearly 3,500 professionals in 28 countries around the world. For more information, visit www.duffandphelps.com.