MARSH

Incidentes cibernéticos

em tempos de pandemia

Marta Helena Schuh
Abril
São Paulo

MARSH & McLENNAN COMPANIES

Sobre Transformação Digital:

Quem acelerou a transformação digital na sua empresa?

Tecnologia e o momento atual

1. A sociedade tem uma dependência aumentada da infraestrutura digital;
2. As empresas precisam implementar o home office sem ter estruturado politicas e processos condizentes e assim flexibilizam acesso e segurança;
3. A dependência de VPNs e outros aplicativos remotos pode não ser suportada pela banda e pode resultar em falha do sistema da infraestrutura da organização ou no provedor de SaaS.
4. A natureza curiosa da psique humana, especialmente em tempos de incerteza;
5. A sociedade passa a consumir serviços on-line,
6. Indivíduos que não são necessariamente "conhecedores de tecnologia" precisam se tornar subitamente acostumados a usar a tecnologia em suas vidas diárias.

Home Office

75% das empresas latino-americanas possuem notebook para trabalhar

35% das empresas não possuem nenhuma politica de segurança definida

30% se conectam em redes de Wi-fi publicas fora do escritório

44% possuem politicas de segurança definidas

8% utilizam VPN

21% desconhecem se existe alguma politica

Fonte: Kaspersky

O resultado...

Buscar

Valor | Empresas

Com pandemia, invasão de sistemas triplica

Sistemas domésticos de trabalhadores em home office geralmente são mais vulneráveis

Por Gustavo Brigatto — De São Paulo

27/03/2020 05h00 · Atualizado há 3 dias

This article is part of our Essential Guide: Essential Guide: Technology readiness for the Covid-19 coronavirus crisis

Coronavirus now possibly largest-ever cyber security threat

The cumulative volume of coronavirus-related email lures and other threats is the largest collection of attack types exploiting a single theme for years, possibly ever

Coronavírus eleva ataques cibernéticos: saiba como proteger privacidade e dados

Hackers se aproveitam de um tema sensível para lançar golpes, roubar dados e extorquir vítimas

EDITORS' PICK | 158.782 views | Mar 23, 2020, 06:10am EDT

COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online

EDITORS' PICK | 20.203 views | Mar 16, 2020, 04:12pm EDT

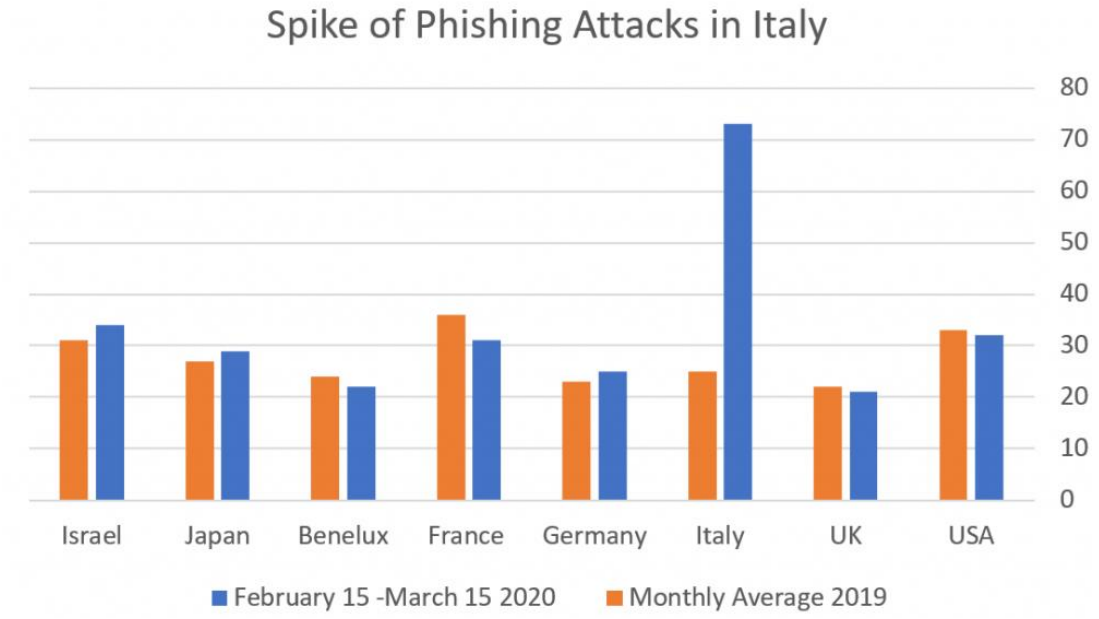
2,500 Attacks In Less Than A Day: Coronavirus Scammers Just Went Into Overdrive

COVID-19: Hackers Begin Exploiting Zoom's Overnight Success to Spread Malware

March 30, 2020 Ravie Lakshmanan

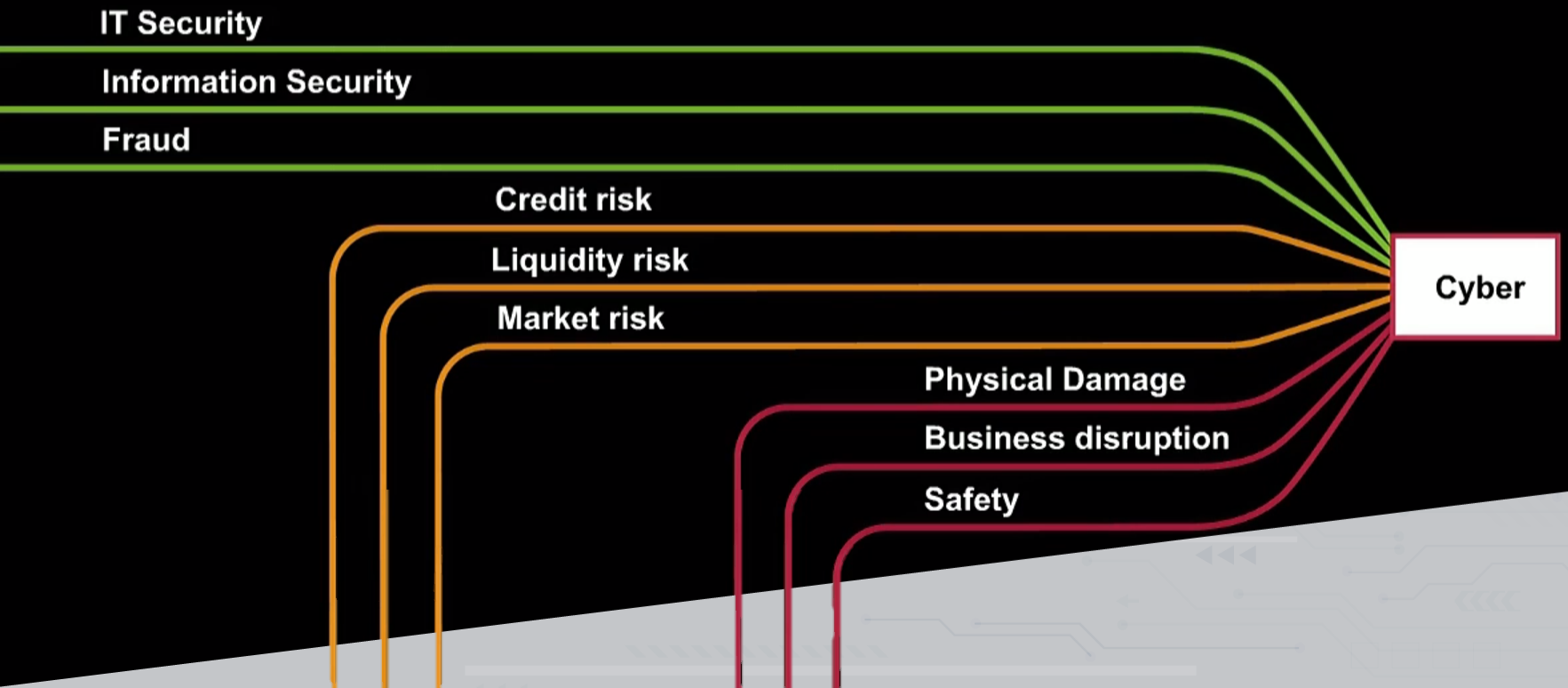
Aumento de Ameaças durante a Pandemia

Segundo a Crypto ID ouve um aumento de **351%** no Brasil, em tentativas de Phishing



https://threatpost.com/cynet-the-coronavirus-is-already-taking-effect-on-cyber-security-this-is-how-cisos-should-prepare/153758/

What is Cyber?



Quais as causas de interrupção dos negócios que mais geram impacto?

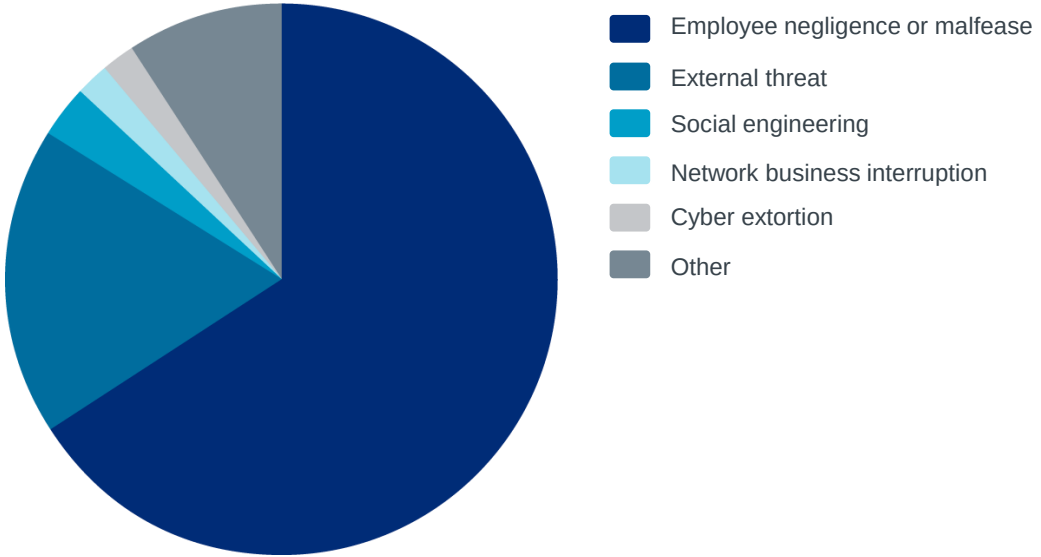
50% Incidentes cibernéticos

40% Fogo, explosões

38% Desastres naturais

28% Falhas de fornecimento

28% Quebra de máquinas



Source: Allianz Global & Specialty. Figures represent the percentage of answers of all participants who responded (947). Figures don't add up to 100% as up to three risks could be selected.

Perdas para a empresa

- Perda de receita
- Despesas emergenciais
- Extorsão cibernética
- Perda / destruição de dados
- Danos a sistemas
- Custos com Pericia digital
- Honorários advocatícios
- Notificações e call centre
- Mídia e danos de imagem
- Multas e Penalizações

Danos a terceiros

- Responsabilidade pela Segurança dos Dados:

1. Contaminação de Dados de Terceiros por software não autorizado ou código malicioso (vírus);
2. Negação de acesso inadequada para o acesso de um Terceiro autorizado aos Dados;
3. Roubo ou furto de código de acesso nas instalações da Sociedade ou via Sistema de Computador;
4. Destruição, modificação, corrupção e eliminação de Dados armazenados em qualquer Sistema de Computador;
5. Divulgação de Dados devido a uma Violação de Segurança de Dados;

- Danos à Propriedade Intelectual

Responsabilidade por danos a marcas registradas ou slogans e direitos autorais

Outros Benefícios

- Time de gerenciamento de crises capacitado, incluindo peritos forense, apoio jurídico, e outros profissionais

Dicas de segurança cibernética para home office #MarshCyber

- Habilite o acesso remoto à rede através de um canal seguro, quando for necessário (p.e. VPN).
- Exija o duplo fator de autenticação, sempre que possível.
- Utilize serviços remotos somente em protocolos seguros (HTTPS).
- Limite os acessos remotos unicamente aos serviços permitidos e a zonas isoladas de rede.
- Valide os controles dos dispositivos (p.e. antivírus, atualizações, configurações de segurança, etc.)
- Valide as capacidades de limpeza e bloqueio remoto nos dispositivos
- Assegure-se de que seus dispositivos sejam criptografados e valide os controles de prevenção de vazamento de informação.
- Realize um backup das informações importantes.
- Conscientização, conscientização e conscientização (p.e. como detectar um phishing, e-mails maliciosos, etc.)
- Informe aos usuários os protocolos para reportar qualquer situação suspeita ou incomum.
- Incremente os níveis de monitoramento de eventos de segurança. Alguns exemplos:
  - Falhas e tentativas de autenticação bem-sucedidas
  - Acesso de um mesmo usuário em múltiplos endereços de IP.
  - Tráfico de rede suspeito.
  - Conexões em localidades incomuns (p.e. países não usuais).
- Aconselha-se evitar o uso de redes públicas ou inseguras para a conexão.

Leve em consideração que a aplicação de políticas de home office podem saturar os acessos à internet. Revise a capacidade e monitore constantemente os acessos para assegurar a continuidade dos serviços.

Marta Helena Schuh, VP
FINPRO, Head Cyber Insurance
marta_schuh@jltbrasil.com