2018

White paper series
Questão 2

GESTÃO DO RISCO
— CIBERNÉTICO NACIONAL —

OEA | Mais direitos para mais pessoas

CRÉDITOS

Luis Almagro

Secretário-Geral da
Organização dos Estados
Americanos (OEA)

Autor principal

Melissa Hathaway

Equipe técnica da OEA

Claudia Paz y Paz
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Bárbara Marchiori de Assis
Nathalia Foditsch
Gonzalo Garcia-Belenguer

CONTENIDO

1

INTRODUÇÃO

Nos últimos 30 anos, os governos, as empresas e os cidadãos se tornaram criticamente dependentes da Internet e das tecnologias da informação e comunicação (TICs). Temos a crença de que sempre funcionarão os serviços essenciais para o cidadão, como a energia e as telecomunicações, e que os bens, serviços, dados e capital cruzarão fronteiras sem inconvenientes. A realidade, no entanto, é que muitos sistemas e infraestruturas em rede são vulneráveis e estão sendo explorados. Organizações de todo tipo estão sofrendo grandes violações em seus dados, atos criminosos, interrupção do serviço e destruição de sua propriedade. Coletivamente, nossa insegurança está crescendo. Mais de 100 países e um número cada vez maior de atores e pessoas não estatais podem causar danos às infraestruturas em rede de governos e da indústria. Os objetivos variam conforme o ator: ativismo político; fraude e delito informático; roubo de propriedade intelectual (PI); espionagem; interrupção de serviço; destruição de bens e ativos. Os países e as empresas estão vivendo em um mundo de insegurança cibernética: todos os governos, empresas e pessoas estão enfrentando riscos cibernéticos. E todos compartilham um grau de responsabilidade em sua gestão. Como evidenciado em eventos recentes, os países e as empresas devem primeiro compreender que no centro de sua estratégia e agenda digital deve estar um enfoque disciplinado de gestão de riscos. O risco da inação é grande demais.

O risco é definido em termos de tempo, quando algo ou alguém está exposto a um perigo, dano ou perda . A condição de risco pode mudar em função das ações realizadas por pelo menos dois atores: o atacante, que obtém e utiliza a capacidade de causar dano, e o objetivo pretendido, que pode tomar precauções para resistir ou frustrar o perigo pretendido pelo atacante. Todos os dias a nossa dependência digital cresce, mas a compreensão dos riscos associados a essa dependência continua sendo incipiente. Ainda assim, o risco cibernético vem aumentando não apenas por estar disponível e ser acessível, mas por estar sendo usado o mercado de software e ferramentas maliciosas, serviços ilícitos e dados sensíveis (não públicos). Por exemplo, é possível comprar software malicioso por um dólar e é possível lançar um ataque distribuído de denegação de serviço por menos de mil dólares. Ataques sofisticados de ransomware (sequestro de arquivos em troca de um resgate) estão disponíveis por duzentos dólares e serviços maliciosos de correio eletrônico não desejado são obtidos por aproximadamente quatrocentos dólares . Inclusive as armas mais sofisticadas dos serviços de inteligência dos governos estão facilmente disponíveis para descarga . Qualquer um que tenha a intenção de utilizar estas capacidades para realizar ataques e causar danos pode ter acesso a elas. Como demonstram os eventos de 2017, governos, empresas e pessoas foram prejudicadas por alguns dos maiores ataques cibernéticos até agora.

Em maio de 2017, o sequestro de arquivos em troca de resgate teve como alvo falhas nos sistemas operativos de Microsoft Windows, afetando milhões de computadores em 150 países, em todos os setores comerciais. Este ataque global, um sequestro de arquivos muito simples chamado WannaCry, paralisou operações de fabricação, sistemas de transporte e sistemas de telecomunicações. De acordo com o Departamento Nacional de Auditoria do Reino Unido, o WannaCry afetou pelo menos 81 das 236 entidades do Serviço Nacional de Saúde inglês, tornando inoperável o equipamento médico e afetando principalmente a saúde e a segurança pública .

Em junho de 2017 foi lançado o NotPetya, outro malware (software mal-intencionado), mais destrutivo. O NotPetya se estendeu às empresas na rede mundial através de um mecanismo de atualização de software para um programa de contabilidade amplamente utilizado (doc.me). Em questão de minutos, o software mal-intencionado infetou dezenas de milhares de sistemas conectados à Internet em mais de 65 países, incluídos alguns pertencentes a instituições governamentais, bancos, empresas de energia e outras companhias. Por exemplo, o ataque do NotPetya contra a A.P. Moller-Maersk, a maior companhia naval do mundo, bloqueou e eliminou os sistemas de tecnologia da informação da empresa no mundo todo. Portanto, a Maersk teve que deter as operações na maioria dos 76 terminais portuários da companhia no mundo todo, interrompendo o comércio

marítimo durante semanas. As perdas financeiras da Maersk causadas pelo NotPetya superaram os $300 milhões, pois teve que reconstruir toda a sua infraestrutura, incluídos 4.000 novos servidores, 45.000 computadores novos e 2.500 aplicações novas . –estima-se que o NotPetya ocasionou perdas de bilhões de dólares devido à interrupção dos negócios e à destruição de propriedade no mundo inteiro . As perdas primárias e secundárias para a economia digital foram significativas e o dano aos serviços e infraestruturas críticas demorou meses para se recuperar.

Ainda mais preocupante, em agosto de 2017 uma instalação de petróleo e gás da Arábia Saudita se viu repentinamente obrigada a fechar. Foi vítima do Trisis, um vírus informático bem projetado para sabotar os sistemas de controle industrial (SCI). Criado para afetar os componentes operativos da tecnologia da informação em sites industriais, como petróleo e gás e serviços de água, este software malicioso, ou arma, tem como objetivo específico os mecanismos de segurança física (sistema de interrupção por emergência) dos SCI. Ainda que este seja apenas um exemplo público da utilização bem-sucedida deste software destrutivo, a Schneider Electric recomendou aos seus clientes de serviços críticos e proprietários de infraestrutura garantir que seus sistemas sejam redundantes em caso de que um ou mais sistemas falhem como resultado de uma atividade maliciosa futura .

As atividades cibernéticas maliciosas de 2017 mostram um extraordinário impacto em termos de perda e dano, mas as ferramentas utilizadas para causar dano realmente não eram sofisticadas. O número de ataques dirigidos contra os sistemas de energia, de telecomunicações, transporte e financeiros quase duplicaram nos últimos cinco anos, uma tendência que apresenta riscos de segurança econômica e nacional para todos. Portanto, existe uma necessidade urgente de que os líderes governamentais e corporativos participem de processos efetivos de gestão de riscos cibernéticos e abordem os riscos digitais em seus processos de planejamento estratégico.

2

MARCOS PARA COMPREENDER O RISCO CIBERNÉTICO

Os países, as organizações internacionais e as instituições acadêmicas estão desenvolvendo marcos para ajudar os líderes governamentais e corporativos a diagnosticar e reduzir o risco cibernético. Estes marcos são imensamente necessários porque, nas últimas três décadas, estes mesmos líderes se convenceram dos supostos benefícios -dadas suas características- das tecnologias de informação comercial, que significam maior produtividade, maior eficiência, menores custos de equipamento, de capital, armazenamento e processamento de dados, e crescimento dos resultados. Portanto, os dirigentes postergaram o investimento em segurança e resiliência de suas infraestruturas de rede e negócios digitais. As atividades cibernéticas destrutivas e interruptivas de hoje em dia exigem que estes líderes enfrentem o fato de que, inadvertidamente, entrelaçaram a insegurança no próprio núcleo da sociedade. As perdas estão se acumulando, o dano está crescendo e o perigo é iminente.

Marcos governamentais

Os governos começaram a desenvolver marcos, pontos de referência e estratégias nacionais mais amplas para melhor compreender suas dependências e as vulnerabilidades de infraestrutura da Internet, e para assegurar as redes nacionais, as infraestruturas e os serviços dos quais dependem seu futuro digital e seu bem-estar econômico. No entanto, quando se trata de mapear e alertar sobre o risco cibernético de um país, a pergunta que fica no ar é: Como diagnosticar e reduzir um risco acumulado durante 30 anos? É importante começar compreendendo o que é o plano estratégico de 3-5 anos de um país e determinar o que pode ser feito para atingir esse objetivo em longo prazo. Por exemplo, os holandeses estimaram que, em 2020, pelo menos 25% do seu produto interno bruto (PIB) estará composto pela economia digital (isto é, bens digitais e serviços eletrônicos). Os Países Baixos afirmaram que seu futuro depende da capacidade de assegurar sua economia digital e estão realizando alguns dos investimentos necessários e reformas estruturais para atingir esse objetivo. Outros países, como os Estados Unidos e a Alemanha, estão identificando as principais companhias que representam mais de 2% do PIB do país e estão trabalhando com elas para garantir que a gestão do risco e a resiliência sejam parte de seus processos gerais de planejamento comercial. A maioria dos outros países, contudo, adotaram um enfoque mais amplo exigindo a proteção das "infraestruturas críticas", ou seja, os ativos, sistemas e redes essenciais, que se considera estão se tornando vulneráveis pela maior interconexão e confiança na Internet, e como tal ficam suscetíveis a falhas nos equipamentos, erros humanos, clima e outras interrupções causadas naturalmente, e a ataques físicos cibernéticos . Neste enfoque, o desafio é que não existe uma delimitação clara entre a responsabilidade do governo e da indústria. Isto faz com que seja difícil responsabilizar alguém em particular pela inação. Enquanto isso, a insegurança da sociedade aumenta à medida que existe a falta de compromisso em reduzir o risco e aumentar a resiliência.

Alguns governos determinaram que é a hora de intervir no mercado e estão utilizando regulações ou leis para exigir que certos setores identifiquem, avaliem e corrijam as deficiências em sua postura de segurança. Os setores regulados incluem: serviços elétricos, serviços financeiros, atendimento em saúde, transporte e telecomunicações. Outras medidas regulatórias que estão sendo adotadas pelos países implicam a obrigação de notificação detalhada e envio de relatórios à autoridade local e/ou nacional em relação a: uma violação que tenha ocorrido e o tipo de dados expostos ou perdidos, técnica ou método utilizado em uma violação e cortes ou interrupções no negócio (telecomunicações) que possam ter ocorrido.

A União Europeia (UE) está impondo este tipo de enfoques preceptivos em suas infraestruturas críticas e operadores de serviços essenciais. Em agosto de 2016, a UE adotou um regulamento intitulado Diretiva de Segurança das Redes e dos Sistemas de Informação (NIS, por suas siglas em inglês) da UE. A regulação estabeleceu regras de segurança cibernética (ou conjuntos de controles de segurança) às empresas que prestam à sociedade serviços que foram categorizados como essenciais. Os serviços cobertos pela regulação incluem energia, transporte, bancos, finanças, água e saúde, bem como serviços digitais, como mercados on-line (por exemplo, eBay, Amazon), motores de busca (por exemplo, Google) e provedores de serviços na nuvem. Os Estados membros da UE têm até maio de 2018 para incorporar o regulamento às suas leis nacionais. A Diretiva NIS exige que os operadores de serviços essenciais nesses países tomem as medidas de segurança apropriadas e notifiquem sua autoridade nacional pertinente (por exemplo, a autoridade competente ou o grupo de resposta a incidentes de segurança informática (CSIRT, por suas siglas em inglês) sobre qualquer incidente cibernético grave). Este enfoque obriga a prestação de contas e pode reduzir o risco cibernético porque está "obrigando" a indústria a tomar medidas para reduzir as vulnerabilidades e aumentar a resiliência.

A China adotou um enfoque semelhante ao da Europa e inclusive incorporou elementos da Diretiva NIS em sua nova lei nacional de segurança cibernética adotada pelo parlamento chinês em novembro de 2016, que entrou plenamente em vigor em 31 de dezembro de 2017. A lei tem sete capítulos e 79 artigos, e é "integral e abrangente" no sentido de que especifica as responsabilidades das agências governamentais relevantes, dos prestadores de serviços de Internet e dos usuários da Internet. A lei estabelece que, em termos gerais, as companhias deverão tomar medidas técnicas e outras medidas necessárias para: garantir que a Internet funcione de maneira segura e estável, atender os incidentes de segurança cibernética de maneira efetiva, evitar as atividades cibernéticas delitivas e manter a integridade, a confidencialidade e a facilidade de uso dos dados de Internet . Esta regulação obriga as empresas a investir em novas salvaguardas e instalar uma série de controles para garantir estas diretrizes. Também conta com um regime de inspeção e auditoria para garantir que as empresas realizem as atividades adequadas de redução de riscos e prestem contas caso seja comprovado que não contam com processos suficientes em operação.

Os Estados Unidos têm se abstido de adotar um enfoque regulatório nesta matéria e, sim, fez uma chamada à indústria para que invista voluntariamente na redução do risco cibernético às infraestruturas e serviços críticos do país. Em fevereiro de 2013, o presidente solicitou ao Instituto Nacional de Padrões e Tecnologia (NIST, por suas siglas em inglês) que desenvolvesse um conjunto de padrões, metodologias, procedimentos e processos que alinhem os enfoques de políticas, negócios e tecnologia para abordagem dos riscos cibernéticos. O Marco para melhorar a segurança cibernética de infraestrutura crítica foi publicado um ano depois, em fevereiro de 2014, e contém um conjunto de padrões voluntários que ajudam as organizações a avaliar, administrar e responder ao risco de segurança cibernética. O marco indica às organizações a avaliação do risco em cinco tópicos: identificar, proteger, detectar, responder e recuperar. De acordo com algumas estimativas da indústria, cerca de 30% das organizações estadunidenses (incluído o governo) vem utilizando o marco como apoio na avaliação de sua postura de risco e para assumir uma maior responsabilidade na proteção de suas redes e dados confidenciais contra intrusos, danos ou destruição . O apêndice deste documento apresenta vários padrões acordados internacionalmente para as categorias de redução de riscos do Marco de segurança cibernética do NIST. No entanto, as lições aprendidas de violações recentes sugerem que as organizações que usam o Marco de segurança cibernética do NIST estão aplicando as categorias com vistas ao cumprimento, ao invés da avaliação contínua do risco. Por exemplo, algumas organizações que avaliaram sua postura de segurança e preparação utilizando o Marco de segurança cibernética do NIST acreditaram que haviam atingindo um nível de maturidade em segurança cibernética, mas acabaram por ser significativamente prejudicadas pelo WannaCry e pelo NotPetya .

Em setembro de 2017, o NIST publicou ajustes a outra de suas publicações sobre o Marco de gestão de riscos para sistemas de informação e organizações: um enfoque do ciclo de vida do sistema para a segurança e privacidade . Este marco recomenda um processo para que as organizações identifiquem ativos de alto valor e sistemas de alto impacto para que possam avaliar melhor o risco operacional. Também proporciona uma estrutura para determinar e selecionar controles de segurança e privacidade e implementar e avaliar a efetividade do controle. O marco destaca a importância do monitoramento contínuo do risco em tempo real e o cumprimento de certo momento dado. Também reconhece que as decisões de gestão de risco são essenciais para as funções comercias e a consecução da missão. Este marco complementa o Marco para aperfeiçoar a segurança cibernética de infraestrutura crítica e, quando tomados em conjunto, podem oferecer às organizações um enfoque mais estratégico para a gestão de riscos

Marcos internacionais

As organizações internacionais também estão opinando no debate sobre a gestão do risco cibernético e estão trabalhando para acelerar a adoção de medidas efetivas de segurança cibernética utilizando seus próprios marcos e recomendações. O debate internacional sobre gestão de riscos surgiu depois das duas fases consecutivas (2003 e 2005) da Cúpula Mundial sobre a Sociedade da Informação (CMSI), uma reunião mundial da comunidade de 'TIC para o desenvolvimento'. Nesse momento, ao menos 170 países resolveram garantir que todos pudessem se beneficiar das oportunidades que as TIC podem oferecer: melhorar o acesso à infraestrutura e tecnologias de informação e comunicação, bem como à informação e ao conhecimento; aumentar a confiança e a segurança no uso das TIC; desenvolvimento e ampliação de aplicações TIC; e alentar a cooperação internacional e regional . Desde então as instituições internacionais embarcaram em um esforço para desenvolver e propagar marcos para gestão do risco das vulnerabilidades das TIC e aumentar a confiança e a participação na economia digital mundial.

Uma das primeiras organizações internacionais a assumir o desafio foi a Organização dos Estados Americanos (OEA). Em 2004, a OEA, através do Comitê Interamericano contra o Terrorismo (CICTE) e de seu Programa de Segurança Cibernética, começou a fomentar o desenvolvimento da agenda de segurança cibernética nas Américas. A OEA coopera com uma ampla gama de entidades nacionais e regionais dos setores público e privado em questões políticas e técnicas, e busca construir e fortalecer a capacidade de segurança cibernética em seus Estados Membros mediante assistência técnica e treinamento, mesas redondas de políticas, exercícios de gestão de crise e intercâmbio de melhores práticas relacionadas com as TIC. A OEA utiliza marcos governamentais e acadêmicos para ajudar a promover a criação de capacidade de segurança cibernética, e vem auxiliando na mudança do diálogo nacional em seus Estados Membros para reconhecimento de que tanto a conexão à Internet como a infraestrutura de TIC que a sustenta devem ser seguras. Se os países não investem por igual na segurança da infraestrutura-chave e na resiliência de seus sistemas, os custos derivados de atividades cibernéticas nefastas afetarão seu crescimento econômico.

Em 2007, a União Internacional de Telecomunicações (UIT), uma agência especializada das Nações Unidas (ONU) responsável pelas questões TIC, anunciou sua Agenda sobre Segurança Cibernética Global (GCA, por suas siglas em inglês) e publicou um marco que fomenta a cooperação e a colaboração com e entre as partes. A GCA contém cinco pilares estratégicos para guiar os países no desenvolvimento de capacidades a fim de abordar a segurança cibernética de maneira responsável. Eles incluem: (1) Medidas legais; (2) Medidas técnicas e procedimentais; (3) Estruturas organizacionais; (4) Desenvolvimento de capacidades; e (5) Cooperação internacional. Este marco foi seguido pelo desenvolvimento da Guia de Segurança Cibernética Nacional da UIT, em 2011, que dá ênfase aos valores, cultura e interesses nacionais como base de qualquer desenvolvimento efetivo da estratégia nacional. Também analisa questões importantes que todo governo deve abordar quando se trabalha para transformar o tema da segurança cibernética de um simples debate/problema técnico a uma área de política nacional estratégica. Com base nestes esforços iniciais, em 2014 a UIT lançou um Índice de Segurança Cibernética Global (GCI, por suas siglas em inglês) para ajudar os países a estabelecer a linha de base e medir seus programas de segurança cibernética diante dos investimentos e programas de outros países. Este índice está destinado a medir o desenvolvimento ou "bem-estar" de um país nas cinco categorias da Agenda sobre Segurança Cibernética Global: medidas legais, medidas técnicas, medidas organizacionais, desenvolvimento de capacidades e cooperação . Esta metodologia e índice foi um dos primeiros marcos internacionais disponibilizados aos líderes nacionais, que lhes servisse para informar o desenvolvimento de sua estratégia nacional e proporcionar um enfoque para medição do risco cibernético em termos não técnicos.

Em 2015, o Conselho da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) adotou e publicou a Recomendação sobre gestão do risco de segurança digital para a prosperidade econômica e social da OCDE , para instruir no desenvolvimento de estratégias nacionais destinadas à gestão da segurança digital e otimização dos benefícios do desenvolvimento econômico e social esperados pela abertura digital. O marco encoraja os países a adotar um enfoque baseado na gestão de riscos e em um marco de oito Princípios de alto nível inter-relacionados, independentes e complementares que incluem (1) sensibilização, aquisição de habilidades e empoderamento; (2) responsabilidade dos interessados; (3) diretos humanos e valores fundamentais; (4) cooperação; (5) avaliação do risco e ciclo de tratamento; (6) medidas de segurança apropriadas e acordes com o risco e a atividade econômica e social em jogo; (7) inovação; e (8) planejamento da preparação e continuidade. A OCDE defende o conceito de que se os líderes implementarem estes oito princípios junto a outros marcos internacionais, os países estariam posicionados para desenvolver melhores políticas (e estratégias) baseadas na gestão digital do risco de segurança. Os oito princípios não são um marco per se, mas sim componentes-chave onde é possível estabelecer ou melhorar os mecanismos de coordenação dentro do governo e com as partes interessadas não governamentais. A OCDE reconhece que a cooperação público-privada é essencial para a redução do risco cibernético.

Em 2018, o Foro Econômico Mundial (FEM) publicou o Caderno de resiliência cibernética para a colaboração público-privada , uma ferramenta destinada a guiar a colaboração público-privada dentro do Estado no desenvolvimento de políticas de segurança cibernética. A Seção 4.7 do Caderno, em particular, aborda a necessidade de estabelecimento de

um marco nacional claro de governança cibernética, que inclua funções, responsabilidades e capacidades que se espera dos setores público e privado. O marco de três níveis proposto pelo FEM tem como objetivo ajudar os governos nacionais a designar responsabilidades e melhor alinhar as funções e responsabilidades específicas com três capacidades de segurança claras: solidez, resiliência e defesa, cada uma fortalecendo as demais. A solidez é definida como "a capacidade de prevenir, repelir e conter ameaças". A resiliência é definida como "a capacidade de administrar e solucionar violações bem-sucedidas". E a defesa é definida como "a capacidade de se adiantar a, interromper e responder a ataques" . Este marco está baseado nas iniciativas que datam do Conselho da Agenda Global FEM 2014 sobre Risco e Resiliência e o Livro Branco de 2016 Compreender o Risco Cibernético Sistêmico. O FEM avançou no diálogo sobre o risco cibernético e fez conexões diretas a impactos econômicos e consequências comerciais da insegurança cibernética.

3

MARCOS DE COMUNIDADE TÉCNICA E A ACADEMIA

As instituições acadêmicas, os grupos de especialistas e a comunidade técnica também começaram a se envolver e propuseram diversas metodologias para acelerar a preparação cibernética e os níveis de maturidade dos países e das organizações.

O Índice de preparação cibernética 2.0 (CRI 2.0, por suas siglas em inglês) , publicado por uma equipe de especialistas do Instituto Potomac para Estudos de Políticas em 2015, está baseado no Índice de Preparação Cibernética 1.0 de 2013, que contribuiu com um marco metodológico para avaliar a preparação cibernética. O CRI 2.0 oferece uma metodologia integral, comparativa e baseada na experiência para avaliar o compromisso e a maturidade dos países para fechar a brecha entre sua postura de segurança cibernética atual e as capacidades cibernéticas nacionais necessárias para respaldar seu futuro digital. O CRI 2.0 usa mais de setenta indicadores únicos através de sete elementos essenciais para discernir atividades operacionalmente preparadas e identificar áreas de aperfeiçoamento nas seguintes categorias: (1) estratégia nacional; (2) resposta a incidentes; (3) delito informático e aplicação da lei; (4) troca de informação; (5) investimento em I+D; (6) diplomacia e comércio; e (7) defesa e resposta a crises. O plano acionável resultante entrega uma folha de rota de redução de riscos como guia para os países. Mas o mais importante é que o CRI 2.0 vincula o crescimento econômico e o desenvolvimento com as políticas de segurança nacional. Também reconhece que para aproveitar todo o potencial da economia na Internet, em termos de crescimento do PIB, maior produtividade e eficiência, maior capacidade de trabalho e um melhor acesso aos negócios e à informação, é necessário alinhar as estratégias de desenvolvimento econômico às prioridades de segurança nacional. Em outras palavras, as TIC só podem gerar crescimento econômico se forem implementadas políticas, processos e tecnologias para proteger e assegurar a infraestrutura e serviços cibernéticos dos quais depende o futuro digital e o crescimento de um país. O CRI 2.0 está centrado nas ferramentas que os líderes globais podem aproveitar, incluindo políticas, legislação, regulações, padrões, incentivos de mercado e outras iniciativas, para proteger o valor de seus investimentos digitais e abordar a erosão econômica em curso, produto da insegurança cibernética.

O Modelo de Maturidade de Capacidade de Segurança Cibernética de Oxford (CMM, por suas siglas em inglês), publicado em 2016 pelo Centro Global de Treinamento de Segurança Cibernética (GCSCC, por suas siglas em inglês) na Universidade de Oxford, apresenta distintos níveis de maturidade de segurança cibernética dos países, em cinco dimensões de capacidade: (1) política e estratégia de segurança cibernética; (2) cultura cibernética e sociedade; (3) segurança cibernética, educação, treinamento e habilidades; (4) marcos legais e regulatórios; y (5) padrões, organizações e tecnologias. Cada uma destas dimensões está dividida em fatores e indicadores mais específicos, que em conjunto são emblemáticos de um Estado mais maduro em capacidade de segurança cibernética. O CMM emprega dois métodos para ajudar a diagnosticar a preparação cibernética. O primeiro método utiliza uma ferramenta de enquete (similar à da UIT), onde um estado pode autodiagnosticar seu estado de preparação. Depois, as respostas da enquete são revisadas e uma equipe participa de um workshop de intercâmbio técnico com partes interessadas-chave do governo, da academia, dos setores público e privado para melhor avaliar a capacidade cibernética em nível estatal em cinco níveis de maturidade cibernética (isto é, nível de início, de formação, estabelecido, estratégico e dinâmico). O CMM da Oxford é uma excelente ferramenta para medir a compreensão das partes interessadas-chave sobre o estado atual da capacidade cibernética e a maturidade do país, apresentando, assim, a base tanto para os objetivos de políticas futuras como para os resultados na redução de riscos.

Finalmente, a Academia de Governança Eletrônico da Estônia lançou um Índice Nacional de Segurança Cibernética (NCSI, por suas siglas em inglês) durante a Conferência de Governança Eletrônica de Tallinn, em maio de 2016, e atualizou/modificou a metodologia para um novo lançamento em janeiro de 2018 . A metodologia incorpora as lições aprendidas pela

Estônia, já que foi um dos primeiros a adotar a governança eletrônica para a sociedade em geral. A versão 2.0 do NCSI inclui doze áreas de capacidades e 46 indicadores para ajudar a avaliar a capacidade de um país, em nível nacional, de construir um estado eletrônico "seguro", que proteja dados e transações ao mesmo tempo em que limita o risco e a exposição digital de um país. Estas doze áreas de avaliação de capacidades são: (1) Capacidade para desenvolver políticas nacionais de segurança cibernética; (2) Capacidade para analisar as ameaças cibernéticas em nível nacional; (3) Capacidade para proporcionar educação sobre segurança cibernética; (4) Capacidade para garantir segurança cibernética de base; (5) Capacidade para proporcionar um ambiente seguro para serviços eletrônicos; (6) Capacidade para prover identificação e assinatura eletrônicas; (7) Capacidade para proteger as infraestruturas críticas da informação; (8) Capacidade para detectar e responder a incidentes cibernéticos 24/7; (9) Capacidade para administrar uma crise cibernética de grande escala; (10) Capacidade para lutar contra os delitos cibernéticos; (11) Capacidade para realizar operações militares de defensa cibernética; e (12) Capacidade para proporcionar segurança cibernética internacional. O NCSI apresenta muitos componentes semelhantes aos dos demais marcos, mas contém seções diferentes que são exclusivas da experiência da Estônia em matéria de governança eletrônica, incluindo como criar um ambiente seguro para serviços eletrônicos e como proporcionar identificação eletrônica e assinaturas eletrônicas.

Resumo dos marcos

Cada marco tem um enfoque ligeiramente diferente, estabelecido para ajudar a fortalecer a postura geral de segurança cibernética de um país e administrar o risco cibernético em nível nacional. Contudo, estes marcos existentes têm muitas características em comum, entre elas: um amplo reconhecimento de que, na era moderna, a segurança nacional e o bem-estar econômico dos países dependem em grande grau da capacidade de assegurar sua infraestrutura cibernética nacional e suas economias digitais; a necessidade de promover a segurança cibernética nos mais altos níveis do governo e da liderança corporativa; a necessidade de começar previamente a proteger as infraestruturas mais críticas e os serviços essenciais; a necessidade de desenvolver marcos legais e regulatórios apropriados para proteger a sociedade contra o delito cibernético, a interrupção do serviço e a destruição de propriedade; a necessidade de que os setores público e privado, bem como as comunidades internacionais e regionais, colaborem para garantir a adoção de estratégias efetivas de gestão de risco cibernético e resiliência; e a obrigação de desenvolver as capacidades nacionais necessárias para aumentar a confiança e a segurança no uso das TIC, corrigir as deficiências e responder a riscos significativos de segurança cibernética.

4

A PREPARAÇÃO CIBERNÉTICA
ADMINISTRAÇÃO DO RISCO

Apesar dos diversos modelos e marcos agora disponíveis aos líderes nacionais para que possam diagnosticar, avaliar e reduzir o risco cibernético de seus países, e as inúmeras chamadas de atenção por parte de profissionais da indústria e especialistas em segurança cibernética, melhorar a segurança cibernética em nível nacional continua sendo um desafio. Por exemplo, os Países Baixos, que reconheceram que sua saúde econômica futura está baseada em uma economia digital confiável e que funcione corretamente, decidiram dedicar fundos suficientes e constituíram um centro para garantir que o país possa atingir seus objetivos de maneira segura. Em julho de 2015, o Coordenador Nacional de Segurança e Contraterrorismo realizou uma Revisão da Política de Infraestrutura Crítica. Nessa revisão, o governo definiu a infraestrutura crítica "como um conjunto de produtos, serviços e processos subjacentes necessários para o funcionamento do país [e que] devem ser seguros e aptos para resistir e se recuperar rapidamente de todos os riscos" . Contudo, quando o porto de Rotterdam -o maior porto da Europa – foi afetado significativamente e seus serviços foram degradados pelo NotPetya em 2017, as autoridades começaram a examinar o estado das dependências de Internet do porto e descobriram que a infraestrutura do porto, na verdade, não havia sido considerado crítica nem em sua estratégia nacional de segurança cibernética nem nas políticas de proteção da infraestrutura.

Inclusive países como o Reino Unido, que identificaram setores críticos específicos -como o atendimento à saúde - que devem cumprir com um padrão de atendimento, não vaticinaram que seus fornecedores de serviços de saúde não estavam dispostos a investir recursos pra manter seu software atualizado e assim proteger os serviços críticos dos pacientes do risco cibernético. Portanto, quando 81 das 236 entidades do Serviço Nacional de Saúde foram vítimas do WannaCry –um simples sequestro de arquivos em troca de um resgate-, um incidente que poderia ter sido evitado facilmente acabou colocando em risco muitas vidas. Como resultado, o Reino Unido foi obrigado a examinar se seu programa cibernético era suficiente e determinar se era necessária uma maior intervenção e atenção do governo para administrar o risco à nação e seus cidadãos.

Como indicado anteriormente, a Alemanha e os Estados Unidos identificaram a porção de empresas que contribuem com pelo menos 2% do PIB do país e, portanto, merecem maior proteção e maior troca de informação/cooperação com o governo. Contudo, a troca de informação entre o governo e a indústria não protegeu as empresas de cair presas da natureza destrutiva do NotPetya. Embora ambos os países possuam processos para compartilhar informação sobre ameaças e inteligência e para "advertir" a indústria de que podem estar vulneráveis aos ataques, neste caso não foi transmitida qualquer advertência iminente. Sendo assim, as empresas com sede em ambos os países foram profundamente afetadas e o comércio eletrônico global enfrentou atrasos de semanas e meses devido à falta de preparação destas companhias e do apoio adequado de seus governos. Finalmente, as principais companhias energéticas da Arábia Saudita, que fornecem quase 25% do gás natural líquido do mundo e alimentam os sistemas de transporte no mundo, ficaram fora de linha devido a outras atividades cibernéticas maliciosas que afetaram tanto os sistemas de transporte como a economia mundial.

Como exemplificam estes casos, nenhum país está ciberneticamente preparado e a preparação deve começar com um enfoque de administração de risco disciplinado. A gestão eficaz do risco requer que os líderes de um país compreendam antes de tudo o que mais valorizam, descrevam o que é o mais importante que devem proteger e demonstrem que estão dispostos a investir o capital político, o tempo dos executivos, o dinheiro e os recursos necessários para protegê-lo.

Por exemplo, a Colômbia iniciou um enfoque de gestão de risco para avaliar sua preparação cibernética e promover a confiança da sociedade no uso do ambiente digital. As gestões foram resposta à tarefa imposta pela Política Nacional de Segurança Digital

(estratégia nacional de segurança digital), que foi aprovada em abril de 2016 pelo Conselho Nacional de Política Econômica e Social (CONPES), mediante emissão do Documento CONPES 3854 de 2016. A Colômbia adotou a guia de gestão de riscos da OCDE e utilizou esse marco juntamente com as recomendações da OEA, da UIT e da Organização do Tratado do Atlântico Norte (OTAN) para avaliar as ameaças digitais ao país e compreender quais ativos críticos estavam em risco . O estudo levou a que o país avaliasse os riscos cibernéticos mais urgentes, identificasse como os incidentes cibernéticos afetam as organizações colombianas, tanto no setor privado quanto no público, e tornasse a segurança cibernética uma prioridade e um componente importante do seu desenvolvimento socioeconômico. Também ajudou a criar consciência entre os diferentes interessados no país sobre os tipos comuns e singulares de incidentes, ameaças e ataques cibernéticos que afetam as entidades e empresas do setor público e começaram a quantificar os custos para a economia do país. A Colômbia reconheceu que a gestão dos riscos cibernéticos em nível nacional é um requisito prévio fundamental para a digitalização do setor e a transformação digital do país.

A experiência da Colômbia evidencia que a gestão do risco começa com a liderança e governança. Como enfatizam a maioria dos marcos, índices e guias publicados por várias organizações intergovernamentais, acadêmicas e comunidades técnicas nos últimos anos, é fundamental a avaliação do que realmente está em risco e a elevação da segurança cibernética ao topo da estratégia de segurança nacional de um país. Entretanto, não é suficiente fazer da segurança cibernética uma prioridade em uma categoria independente e tratá-la como um problema predominantemente de segurança nacional. De fato, a garantia da segurança cibernética também está estreitamente relacionada com a conectividade à Internet e a rápida adoção das TIC que, quando seguras e resistentes, podem levar ao crescimento econômico e prosperidade. Portanto, o alinhamento das iniciativas econômicas com a segurança, o desenvolvimento e a resiliência (a avaliação do valor em risco e o estabelecimento de uma estratégia nacional que maneje as atividades de redução de riscos) é igualmente importante.

Avaliação do risco

Os líderes nacionais devem expressar claramente sua intenção de aproveitar o ambiente digital aberto para a prosperidade econômica e social mediante redução do nível geral de risco de segurança digital dentro e fora das fronteiras. Devem ter consciência de que o risco muda com o tempo em função das ações realizadas por pelo menos dois atores: o atacante, que obtém e utiliza a capacidade de causar dano, e o objetivo pretendido, que pode tomar precauções para resistir ou frustrar o perigo pretendido pelo atacante. Os líderes nacionais devem demonstrar seu compromisso de reduzir os riscos e aumentar a resiliência realizando avaliações contínuas de riscos tanto em nível nacional quanto setorial e adotando medidas, políticas e processos apropriados para administrar os riscos identificados.

Para atingir estes objetivos gerais, os líderes nacionais, os responsáveis pela formulação de políticas e outras partes interessadas relevantes de cada país devem trabalhar juntos para avaliar o risco. O planejamento estratégico e a reflexão podem ajudar a determinar o estado de preparação:

- Qual é a estratégia em curto e longo prazo para o país, incluídas as políticas industriais, os objetivos econômicos e as prioridades de segurança nacional?

- O que poderia colocar estes objetivos em risco? Em outras palavras, quais pontos francos poderiam ser explorados (ou seja, ativos de alto valor não contabilizados) e que poderiam interromper a execução destes objetivos?

- Existem linhas claras de responsabilidade e prestação de contas para garantir a implementação dos objetivos do país e a implementação de medidas de redução de riscos?

- As considerações de segurança cibernética e a resiliência têm sido uma parte central do processo de planejamento?

Esta avaliação exaustiva e abrangente destacará as dependências digitais mais críticas de um país (por exemplo, empresas, serviços, infraestruturas e ativos) que, em caso de dano, trariam graves consequências econômicas e de segurança nacionais. Apenas depois de identificar adequadamente o que é vulnerável, o que poderia colocar em perigo as "joias da coroa" de um país e a probabilidade de que elas estejam expostas a perigos, danos ou perdas, os tomadores de decisões poderão tomar medidas corretivas para frustrar ou reduzir esses riscos.

5

REDUÇÃO DO RISCO ATRAVÉS DE UM PLANEJAMENTO CUIDADOSO

Uma vez realizada a avaliação de riscos, um país pode elaborar um plano de redução de riscos para fechar a brecha entre sua postura de segurança cibernética atual e as capacidades cibernéticas nacionais necessárias para corrigir as deficiências e apoiar as futuras prioridades econômicas e de segurança do país. Os esforços de redução de riscos devem ser dirigidos por uma autoridade nacional de segurança cibernética competente e dedicada: um líder (tanto uma pessoa como uma entidade) que tenha sido promovido e que esteja fortemente ancorado ao mais alto nível do governo para dirigir, coordenar ações e monitorar a implementação do plano e ser responsável pelas deficiências e resultados obtidos. Dado que a segurança cibernética é transversal a muitas áreas de problemáticas diferentes (por exemplo, diretos humanos, desenvolvimento econômico, comércio, controle de armas e tecnologias de dupla utilização, segurança, estabilidade e paz e resolução de conflitos), é importante garantir que a autoridade nacional competente tenha a autoridade posicional, a responsabilidade e o empoderamento para envolver e dirigir tantas partes interessadas, como seja necessário.

Ainda que os lineamentos sobre atividades de redução de riscos sejam abundantes, como demonstram os diversos marcos descritos em seções anteriores, os líderes nacionais deveriam fazer um esforço maior para compreender o panorama do risco cibernético e as ameaças específicas à suas infraestruturas em rede, que deveriam estar claramente delineadas em suas estratégias de segurança cibernética nacional e na(s) avaliação(avaliações) de riscos cibernéticos. E depois deveriam trabalhar com todas as partes interessadas para planejar melhor suas defesas e designar melhor os recursos humanos e financeiros para minimização desses riscos. Estratégias comuns para a mitigação eficaz do risco cibernético incluem:

- Comunicar o que está em jogo e melhorar a conscientização geral sobre os riscos em todos os níveis, desde os líderes governamentais até os cidadãos comuns. As pessoas não podem avaliar a segurança sem antes compreender qual parte de suas atividades diárias está em risco, não só informação pessoal. Portanto, o governo deveria iniciar uma campanha nacional de conscientização pública, promover a educação, o treinamento e o desenvolvimento de habilidades, e empoderar seus cidadãos para que façam parte da solução na construção de uma sólida cultura de segurança cibernética.

- Identificar, priorizar e enfocar os recursos necessários em ativos de alto valor e sistemas de alto impacto que requeiram maiores níveis de proteção: as dependências digitais mais críticas do país (por exemplo, empresas, infraestruturas, serviços e ativos); compreender as vulnerabilidades dos mesmos e priorizar medidas de segurança apropriadas e conformes com o risco econômico e social.

- Desenvolver marcos legais e reguladores apropriados pra proteger a sociedade contra o delito cibernético, a interrupção do serviço e a destruição da propriedade.

- Usar uma ampla gama de ferramentas que incluam políticas, legislação, normas, padrões, incentivos de mercado, esquemas voluntários de cumprimento e outras iniciativas para aumentar a confiança e a segurança na utilização das TIC, bem como corrigir as deficiências nos processos e produtos (por exemplo, Diretiva NIS, Lei de Segurança Cibernética da China, Marco NIST).

- Melhorar o conhecimento da situação, os indicadores de ameaça e as advertências mediante o monitoramento contínuo das ameaças à sociedade interconectada e a utilização das últimas tecnologias para detectar, repelir e conter tais ameaças.

• Desenvolver as capacidades nacionais necessárias para aumentar a preparação, fazer o planejamento de continuidade e responder e se recuperar dos riscos significativos de segurança cibernética quando eles surjam (por exemplo, uma crise cibernética de grande escala).

• Envolver a comunidade internacional para melhorar a segurança geral, a confiabilidade e a resiliência das redes interoperáveis (por exemplo, financeiras, telecomunicações, energia, etc.) através do desenvolvimento de padrões de segurança global e da promoção de acordos multilaterais.

• Antecipar os avanços tecnológicos futuros e avaliar como eles podem introduzir novas vulnerabilidades no país ou, por outro lado, como poderiam virar oportunidades de criação de segurança, fiabilidade e resiliência adicionais nas infraestruturas e ativos da próxima geração

A efetiva implementação destas tarefas e outras atividades requererá a definição e o claro esclarecimento das funções, responsabilidades, processos, direitos de decisão e mecanismos de prestação de contas. Os resultados bem-sucedidos serão beneficiados com o estabelecimento de metas de desempenho para vários departamentos ministeriais ou governamentais, instituições ou pessoas responsáveis por tarefas específicas no plano de ação.

Evidentemente, as atividades de redução de riscos também requerem a destinação de recursos dedicados e apropriados para sua implementação. Fontes e mecanismos de financiamento ineficientes podem tanto minar os resultados pretendidos e reduzir a responsabilidade das entidades encarregadas da segurança cibernética da nação, como deixar recursos insuficientes para a realização de suas próprias missões. Os recursos devem ser definidos em termos de dinheiro (isto é, orçamento dedicado), pessoas, material, bem como de relações e associações necessárias para uma execução e resultados bem-sucedidos dos planos de mitigação de riscos. A alocação de recursos para os objetivos e tarefas dentro de uma estratégia nacional de segurança cibernética não deve ser vista como uma iniciativa a ser tomada uma única vez. O financiamento suficiente, consistente e contínuo proporciona as bases para uma postura nacional eficaz de segurança cibernética. Os recursos podem ser alocados por tarefa ou objetivo, ou por entidade governamental. O governo também pode considerar a constituição de um orçamento central para segurança cibernética, administrado por um mecanismo central de governança de segurança cibernética. Seja juntando diferentes fontes de financiamento em um programa coerente e integrado ou criando um orçamento intragovernamental unificado, o programa geral deve ser gerenciado e monitorado por marcos e prazos claramente definidos para garantir a implementação bem-sucedida da estratégia.

Avaliação contínua do risco

Quando as gestões de segurança cibernética se tornam uma avaliação pontual (seguindo um marco de cumprimento), ao invés de avaliar o risco de forma contínua, elas falham. A gestão de riscos requer uma antecipação proativa das ameaças e uma avaliação contínua das vulnerabilidades dentro das dependências digitais mais críticas do país (por exemplo, empresas, infraestruturas, serviços e ativos). Como indicado anteriormente, existe uma série de marcos que destacam a importância da avaliação contínua do risco e a correção das falhas de controle. O monitoramento e medição do desempenho e a execução bem-sucedida das iniciativas de segurança cibernética (atividades de redução de riscos) devem ser parte dos mecanismos de governança que um país estabelece em sua arquitetura nacional de segurança cibernética. A avaliação contínua do plano de implementação (ou seja, o que está funcionando bem e o que não está) ajuda a instruir ajustes e uma maior defesa da estratégia global. Os mecanismos de boa governança delineiam a responsabilidade e a prestação de contas para garantir uma execução bem-sucedida, e devem ser usadas métricas ou indicadores-chave de rendimento (KPI, por suas siglas em inglês) acionáveis, repetíveis, significativos e dependentes no tempo para reforçar objetivos e cronogramas realistas. As métricas ou indicadores-chave de rendimento devem atender os seguintes critérios:

- ***Serem específicos*** – ter como objetivo uma área específica de melhoramento.
- ***Serem mesuráveis*** – quantificar, ou pelo menos sugerir, um indicador de progresso.
- ***Serem alcançáveis*** – estabelecer quais resultados podem ser obtidos de forma realista, dados os recursos disponíveis.
- ***Serem acionáveis*** — indicar claramente as ações que serão implementadas.
- ***Haver responsáveis*** – especificar quem o fará.
- ***Estarem em função do tempo*** – especificar quando os resultados podem ser obtidos.

Ainda que nenhum país esteja totalmente preparado ciberneticamente e os riscos cibernéticos não possam ser completamente eliminados, eles podem e devem ser administrados. A preparação e a capacidade de reação cibernética começam com um enfoque de gestão de riscos efetivos que inclui uma compreensão clara dos ativos de alto valor e os sistemas de grande impacto do país que requerem maiores níveis de proteção: as dependências digitais mais críticas do país (por exemplo, empresas, infraestruturas, serviços, e ativos). Uma vez compreendido isto, é possível definir e priorizar as medidas de segurança necessárias mediante uma análise de risco e uma avaliação de vulnerabilidade para corrigir as deficiências que são apropriadas e acordes com o risco econômico e social.

Somente com um esforço concertado e coordenado entre os interessados nacionais será possível reduzir significativamente o risco cibernético e avançar para garantir a segurança e a proteção futura de uma nação.

6 CONCLUSÃO

Nossa insegurança cibernética está crescendo. O volume, escopo, escala e sofisticação das ameaças cibernéticas aos serviços e infraestruturas críticas das nações estão superando as medidas defensivas. As atividades cibernéticas destrutivas e interruptivas de hoje em dia requerem que os governos abordem e invistam urgentemente para fazer com que seu país passe de um estado de insegurança cibernética a um estado de preparação cibernética. As perdas estão se acumulando, o dano está crescendo e o perigo é iminente.

Os líderes nacionais devem elaborar estratégias integrais de segurança cibernética nacional que incluam uma autoridade competente e dedicada, responsável pela postura nacional geral de segurança cibernética do país. Deve ser desenvolvida uma compreensão nacional dos riscos enfrentados em todos os níveis, desde os líderes governamentais até os cidadãos comuns. Todos devem compreender as vulnerabilidades do ambiente digital do país e conhecer seu papel na mitigação desses riscos. Esta folha de rota estratégica permite a adoção de medidas, políticas e processos apropriados para corrigir as deficiências e reduzir os riscos à sociedade, à economia e à nação. Isto não é possível de ser conseguido sem recursos dedicados e apropriados que financiem iniciativas para reduzir riscos e aumentar a resiliência. A adoção de uma estratégia nacional de segurança cibernética é um dos passos mais importantes para garantir a infraestrutura e os serviços cibernéticos nacionais dos quais depende o futuro digital e o bem-estar econômico de uma nação moderna.

7

SOBRE A AUTORA

Melissa Hathaway é uma das principais especialistas em políticas de ciberespaço e segurança cibernética. Trabalhou em duas administrações presidenciais dos EEUU, dirigindo a Revisão de políticas do ciberespaço para o presidente Barack Obama, e liderou a Iniciativa Nacional Integral de Segurança Cibernética (CNCI, por suas siglas em inglês) para o presidente George W. Bush. Como presidente da Hathaway Global Strategies LLC, ela assessora clientes do setor público e privado e oferece uma combinação única de experiência técnica e de políticas, bem como experiência em juntas diretivas para ajudar a outros a compreender melhor a transversalidade das políticas governamentais, o desenvolvimento de tendências tecnológicas e da indústria, e os impulsores econômicos que impactam a estratégia de aquisição e desenvolvimento de negócios neste campo. Desenvolveu uma metodologia única para avaliar e medir o nível de preparação para certos riscos de segurança cibernética, conhecido como o Índice de Preparação Cibernética (Cyber Readiness Index 2.09 que pode ser encontrado em: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index. Ela regularmente faz publicações sobre assuntos de cibernética que impactam companhias e países. A maioria de seus artigos podem ser encontrados nos seguintes sites:
www.belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html y
www.ctm.columbia.edu/people/melissa-hathaway.

8

REFERÊNCIAS

1. Dicionário Oxford. O NIST SP 800-30 (Rev A) define o risco como segue: Risco = Ameaça x Vulnerabilidade. O CRM define as declarações de risco como: Risco = Condição (Probabilidade) + Consequência (Impacto).

2. Nicolas Rapp e Robert Hackett, "A Hackers Toolkit". Fortune Magazine 25 October 2017, http://fortune.com/2017/10/25/cybercrime-spyware-marketplace/

3. Eduard Kovaks, "Shadow Brokers Want $20,000 for Weekly Leaks," Security Magazine, 30 May 2017, https://www.securityweek.com/shadow-brokers-want-20000-monthly-leaks; e
Eduard Kovaks, "Shadow Brokers Promise More Exploits for Monthly Fee," Security Magazine, 16 May 2017, https://www.securityweek.com/shadow-brokers-promise-more-exploits-monthly-fee; and
Nicole Perloth, "A Cyberattack the 'World Isn't Ready For,'" The New York Times, 22 June 2017, https://www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html?_r=0

4. National Audit Office, "Investigation: WannaCry cyber attack and the NHS," 27 October 2017, https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

5. Richard Chirgwin, "IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz," The Register, 25 January 2018, https://www.theregister.co.uk/2018/01/25/after_NotPetya_maersk_replaced_everything/

6. O NotPetya interrompeu negócios e destruiu ativos de capital corporativo em nível mundial Os relatórios públicos da A.P. Moller-Maersk, Balersdorf, DHL, DLA Piper, Federal Express, Merck, Mondolez, Nuance, Reckitt Benckiser Group, Rosneft, Saint Gobain, e WPP mostram perdas de pelo menos $2.500 milhões. Um relatório recente da Lloyds of London adverte que um ataque cibernético bem executado poderia causar danos no mundo inteiro, no valor de $53.100 milhões a $121.400 milhões. Veja: Lloyds of London, "Extreme Cyber-Attack Could Cost as Much as Superstorm Sandy," 17 July 2017, https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report.

7. Kelly Jackson Higgins, "Schneider Electric: TRITON/TRISIS Attack Used 0-Day Flaw in its Safety Controller System, and a RAT," Dark Reading, 18 January 2018, https://www.darkreading.com/vulnerabilities–threats/schneider-electric-triton-trisis-attack-used-0-day-flaw-in-its-safety-controller-system-and-a-rat/d/d-id/1330845.

8. Os domínios de nível superior (por exemplo, .mil, .com, .edu, .gov) foram introduzidos em 1985 e permitiram estabelecer o marco para o comércio eletrônico global. A inovação continuou introduzindo novas tecnologias como a criação de linguagem de marcado de hipertexto (HTML) em 1990, que permitiu uma maior troca de informação e de fácil uso na Internet, que finalmente se converteu na World Wide Web. Surgiram outros avanços tecnológicos como: mensagens SMS (1992), protocolo de voz sobre Internet (1996), WiFi (1997), Wikipédia (2001), o buscador de Google (1997), tecnologia de redes sociais (2002) e voz e vídeo sobre Protocolo de Internet com Skype (2003). O setor privado está impulsionando a inovação e doação da tecnologia prometendo reduzir custos, aumentar a produtividade e a usabilidade do consumidor, sem falar muito sobre a segurança. Veja: Melissa Hathaway, "Falling Prey to Cybercrime: Implications for Business and the Economy," in Securing Cyberspace: A New Domain for National Security, February 2012, Aspen Institute Press.

9. Muitos países têm diferentes definições das infraestruturas críticas. Para os fins deste documento, utilizou-se uma definição ampla. Veja: Homeland Security Digital Library, "Presidential Decision Directive 63, PDD/NSC-63," 22 May 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm.

10. Os oficiais anda não definiram quantos setores serão incluídos no escopo da lei. Contudo, muitos especialistas acreditam que esta lei inclui os mesmos setores que a Diretiva de Segurança das Redes e Sistemas de Informação da UE (por exemplo, energia, transporte, bancos, infraestruturas do mercado financeiro, infraestruturas digitais, saúde e água). Veja: Yanqing Hong, "The Cross-border Data Flows Security Assessment: An Important Part of Protecting China's Basic Strategic Resources," 20 June 2017, Yale Law School, Paul Tsai China Center Working Paper, https://law.yale.edu/system/files/area/center/china/document/dataflowssecurity_final.pdf.

11. NIST, "Cybersecurity 'Rosetta Stone' Celebrates Two Years of Success", 18 February 2016, www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success.

12. Hathaway Global Strategies LLC. Insights from engagement with Board of Directors and Management of affected companies.

13. NIST, "NIST Special Publication 800-37 (Rev. 2) DRAFT — Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy (Discussion Draft)," September 2017, https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf.

14. WSIS, Geneva 2003 - Tunis 2005, "Tunis Commitment," 18 November 2005, http://www.itu.int/net/wsis/docs2/tunis/off/7.html.

15. ITU (2014), Global Cybersecurity Index, www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

16. OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

17. WEF (2018), Cyber Resilience Playbook for Public-Private Collaboration, pp. 33-36, https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration.

18. Ibid.

19. O Cyber Readiness Index 2.0 está baseado no anterior Cyber Readiness Index 1.0, que proporcionou um marco metodológico para avaliar a preparação cibernética em cinco elementos essenciais, a saber: estratégia cibernética nacional, resposta a incidentes, delito eletrônico e capacidade legal, troca de informação e investigação e desenvolvimento cibernético. O Cyber Readiness Index 1.0 aplicou esta metodologia a um conjunto inicial de trinta e cinco países. Para obter maiores informações sobre o Cyber Readiness Index 1.0, veja: Melissa Hathaway, "Cyber Readiness Index 1.0," Hathaway Global Strategies LLC (2013), http:// belfercenter.ksg.harvard.edu/ les/ cyber-readiness-index-1point0.pdf.

20. NCSI, "NCSI Methodology," http://ncsi.ega.ee/methodology (1.0) and http://ncsi.ega.ee/ncsi-methodology-2-0-launched/ (2.0).

21. National Coordinator for Security and Counterterrorism, "Review of Policy on Critical Infrastructure," July 2015; and Melissa Hathaway and Francesca Spidalieri, "The Netherlands Cyber Readiness at a Glance," May 2017, Potomac Institute for Policy Studies, http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf.

22. OAS, MINTIC, IDB (2017), Impact of Digital Security incidents in Colombia 2017, https://publications.iadb.org/handle/11319/8552.

OEA | Mais direitos para mais pessoas

GESTÃO DO RISCO CIBERNÉTICO NACIONAL

White paper series
Questão 2

2018