A ilusão de controle e o desafio de uma empresa digigtal adaptável

A instabilidade da sociedade em geral, o aumento na interconexão de dispositivos e a contínua demanda dos clientes por novas experiências sustentam o cenário operacional das organizações modernas. Por causa do aumento do fluxo de informações pessoais e organizacionais, as organizações estão criando e desenvolvendo novas proposições de valor que mudam a maneira como elas fazem as coisas e permitem o desenvolvimento de novos produtos e serviços em ecossistemas de negócios digitais, aproveitando as principais capacidades dos seus aliados estratégicos.[1]

Esse novo normal das empresas de hoje e da sociedade em geral, com maior interconexão entre o físico, o lógico e o biológico, apresenta uma mudança de paradigma que vai além de entender causa e efeito. Isso abre possibilidades de reconhecer a dinâmica global com base em relacionamentos entre elementos que definem os comportamentos dos sistemas, sejam políticos, econômicos, sociais, tecnológicos, legais ou ambientais. Portanto, para entender as propriedades inerentes de um sistema e explorar as propriedades emergentes que se manifestam em razão da própria dinâmica do sistema, é necessário desenvolver uma forma sistêmica de pensar que leve em conta o fluxo de interconexões visíveis e invisíveis.[2]

Proteger a proposição de valor das organizações no ambiente atual não é um exercício de mitigação ou prevenção de eventos adversos, mas sim da redução do impacto do que não é entendido ou não pode ser previsto. Essa distinção é necessária para superar a ilusão de controle e a falsa sensação de segurança derivada das tentativas geralmente fúteis e desesperadas das organizações de prever instabilidades sociais e econômicas, que podem, no final, afetar a própria dinâmica da organização.[3]

A administração de risco empresarial deve estar posicionada para lidar com as incertezas, transferindo a atenção voltada para evitar falhas, que são inevitáveis, para entender o controle como um equilíbrio dinâmico entre reduzir as incertezas (ou seja, risco conhecido, aplicação de controles conhecidos) e ampliar novos comportamentos emergentes (ou seja, risco latente e emergente, design e execução de cenários e simulações). O objetivo deve ser reimaginar integralmente o que mais pode dar errado, criar uma postura vigilante e determinar uma forma de melhor responder a todos os tipos de ameaças.[4]

Além disso, ajuda também analisar a ilusão de controle da gestão de risco cibernético nas organizações, como superar isso à luz da natureza dinâmica do risco, e ainda reconhecer as falhas dos executivos para entender e administrar o risco cibernético. Entender as estratégias digitais que são configuradas e instaladas no atual ambiente de inovação e crises tecnológicas demanda assumir risco na estrutura de limiares definidos, acordados e simulados pela organização.

Por que o Controle é uma Ilusão?

Talvez o cenário mais desejado pelos humanos seja a sensação de manter as coisas dentro de um espectro de variação conhecido e validado. É natural querer a paz de espírito que vem quando se sabe que uma ação equivalente pode ser repetida no futuro com resultados semelhantes àqueles experimentados inicialmente. As pessoas têm necessidade de prever resultados com base em experiências anteriores e ver os comportamentos esperados se materializarem, de forma que possam manter suas agendas e definir planos para atingir metas específicas.[5]

No entanto, quando a alta direção está comprometida com esse tipo de perspectiva, com base em alguns sucessos reconhecidos de suas propostas e estratégias, ela costuma assumir uma postura arrogante e supervalorizar a experiência, que pode levar a escolher investimentos com base em eficiência e não na capacidade da organização para adaptação e flexibilidade, quando as coisas não andam conforme planejado. Essa situação geralmente cria tensão com as equipes de risco, que precisam aceitar as disposições executivas sem maiores objeções, com base em um exercício de comando e não em um exercício de reflexão, desafio e orientação que leva em conta a potencial

JEIMY J. CANO M. | PH.D., ED.D., CFE, CICA

Possui mais de 25 anos de experiência como executivo, acadêmico e profissional de segurança da informação, segurança cibernética, computação forense, crime digital e auditoria de TI. Em 2016, ele foi indicado como Educador de segurança cibernética do ano para a América Latina. Publicou mais de 250 artigos em vários periódicos e apresentou trabalhos em eventos do setor no nível internacional.

volatilidade, a instabilidade e a incerteza do ambiente.

Especificamente, as equipes executivas tentam simplificar suas perspectivas sobre risco criando uma estrutura de risco definida, relatórios de referência de outras organizações no seu setor comercial, e uma visão geral de como outros lidaram com esse risco. Isso pode levar a um viés de influência,[6] que resulta de igualar a experiência de outros com a dinâmica particular da organização, gerando uma falsa sensação de segurança. Essa posição pode levar a pontos cegos na organização e pode possibilitar novos espaços para que adversários criem situações que estejam fora do radar dos exercícios executados pelo conselho diretor (board of directors - BoD) e a equipe de risco da organização.

Em geral, controle é entendido nas organizações como um exercício de limitação de incertezas através da restrição de condições concretas para permitir uma estrutura conhecida de ações com resultados esperados e administráveis. Quanto mais conhecidas forem as incertezas, melhor serão as capacidades de mobilização e projeção da organização. Na medida em que os dados anteriores e os dados disponíveis de pares oferecem perspectivas melhores e maiores, o apetite pelo risco crescerá. Assim, maiores desafios serão assumidos pela organização, sem avaliar as capacidades atuais e implementar atualizações necessárias para tratar do que não estiver de acordo com o plano.[7]

Tomar decisões baseadas apenas nos critérios de limitação de incertezas e com dados dos eventos anteriores cria uma falha que torna as organizações mais suscetíveis a surpresas desagradáveis. O resultado é pouca ação ou nenhuma margem para ação, o que leva a perda de reputação com clientes em razão da falta da capacidade de preparo e resposta. Quando ocorre um evento infeliz, cria-se um dilema de controle que limita a discrição e a autonomia das áreas de negócios (que conhecem o terreno em primeira mão) para agir. Em vez disso, os executivos de mais alto escalão são os que elaboram uma solução que devolve o controle para a organização e dá paz de espírito para o conselho diretor (board of directors - BoD) e suas partes interessadas.[8]

No entanto, o controle não se restringe apenas a seguir o plano ou a estratégia estabelecida (em momento e lugar específico, de maneira específica). Em vez disso, controle significa manter o curso e ajustar-se às condições do ambiente, criando cenários diferentes que permitam repensar as ações e a ampliação de opções para lidar com as instabilidades que surgirem. Dessa forma, a organização não pode só realizar o que ela quer, mas também criar uma base de aprendizados essenciais que ajudarão a atualizar suas capacidades para enfrentar novas incertezas.[9]

Tomar decisões baseadas apenas nos critérios de limitação de incertezas e com dados dos eventos anteriores cria uma falha que torna as organizações mais suscetíveis a surpresas desagradáveis.

A Ilusão de Controle de Risco Sistêmico

O risco cibernético reside nas interconexões e nas interações de vários componentes configurados por pessoas, processos, tecnologia e normas. Essas interconexões e interações são um ecossistema dinâmico que mantém um fluxo de informação que é usado para definir o estado de proteção e operação das iniciativas que surgem em um contexto digital. Não é a conformidade regulatória prevista para fatores de risco conhecidos, mas o reconhecimento da sua instabilidade e mutabilidade que permite que as capacidades necessárias sejam alinhadas e coexistam com as violações que ocorrerão.[10]

Como o risco cibernético é sistêmico, sua materialização exige uma análise de contágio do referido risco (ou seja, uma análise do efeito cascata derivado do nível observado de acoplamento e de interações). Essa análise determina a capacidade de resposta e sensibilidade da organização

diante de eventos instáveis ou incertos que comprometem seu funcionamento e o nível de impacto dos objetivos estratégicos da organização. A materialização do risco cibernético é um desafio para o modelo de maturidade da segurança cibernética da organização diante de mudanças externas e internas que a organização encontra, e revela pontos cegos no seu modelo de segurança e controle.[11]

Se a administração de risco cibernético for entendida com um exercício para limitar a exploração de vulnerabilidade, prevenir ataques e mitigar a materialização de risco, então as organizações trabalharão na sua zona de conforto de conformidade com a aplicação de normas e padrões, entendendo a incerteza e a instabilidade como seus inimigos e, portanto, participando de uma cruzada em que as certezas serão escassas e as surpresas serão notícia constante para o conselho diretor. Ao adotar essa perspectiva, as organizações manterão sempre uma postura de vítima que não oferece margem para recuperação e aprendizado, dando ao adversário a vantagem de ter a incerteza como fator fundamental na execução de suas ações.[12]

Quando o risco cibernético é entendido como parte da dinâmica da organização e suas relações dentro do ecossistema de negócios digitais, entende-se então que é necessário não só reduzir a incerteza e a instabilidade, mas também aumentar a capacidade da organização aprender e superar ataques bem sucedidos. Nesse sentido, é importante focalizar a evolução do risco e atualizar as capacidades de segurança cibernética, que provoca a deterioração da capacidade de inteligência do adversário, gerando maior incerteza no modelo de risco do adversário. É também necessário estudar os efeitos cascata da materialização desse risco, com resiliência como um fator fundamental para dar conta da instabilidade e o caos gerados por um evento adverso bem-sucedido.[13]

As Sete Falhas dos Executivos

Os executivos de hoje acham que o risco cibernético é um tópico importante porque muitos ataques cibernéticos de alta visibilidade, geralmente em infraestruturas críticas, resultaram em consequências para os gerentes de organizações, especialmente em relação às suas responsabilidades de monitoramento e garantia do risco exigidas não apenas pelos comitês de auditoria, mas também pelos supervisores de cada um dos setores de negócios da organização.[14]

Para lidar com esse risco, os gerentes acostumados com a inércia da tradicional administração de risco acabam

É importante focar na evolução do risco e atualizar as capacidades de segurança cibernética, que provoca a deterioração da capacidade de inteligência do adversário, gerando maior incerteza no modelo de risco do adversário.

tratando o risco cibernético como um risco a mais para a organização, particularmente associado a questões tecnológicas, o que significa tratá-lo como um risco conhecido com controles que são claramente verificáveis. Isso é como apostar no resultado de um cenário que é, por definição, incerto, o que demonstra desconhecimento, é possivelmente irresponsável, e demonstra falta de cumprimento do dever primordial dos executivos, o dever de diligência. Isso, em última instância, compromete as iniciativas da organização e sua capacidade de responder.[15]

Nesse sentido, os executivos de nível C devem ficar vigilantes para reconhecer e superar as sete transgressões que são geralmente cometidas ao confrontar o desafio da administração de risco cibernético relevante e adequado para a organização.

1. **Pensar que podem prever eventos extremos**—É mais eficiente focalizar as consequências e avaliar o impacto de eventos extremos.
2. **Estudar o passado para administrar o risco atual e futuro**—O mundo de hoje não parece com o passado. Interdependências e não linearidades aumentaram.
3. **Ignorar conselhos sobre o que não fazer**—Uma organização pode ser bem sucedida evitando perdas enquanto seus rivais tentam vencer.
4. **Assumir que o risco pode ser medido por desvios padrão**—Não existe aleatoriedade domesticada. As mudanças não se movem dentro de certos limites.
5. **Deixar de perceber o que é matematicamente equivalente não é psicologicamente equivalente**—É possível ser enganado pela matemática ou pela estrutura de apresentação do risco.
6. **Acreditar que eficiência e maximização do valor do acionista não tolera redundância**—A maioria dos executivos não percebe que a otimização torna as organizações vulnerável a mudanças do ambiente porque geralmente envolve não ter capacidades

duplicadas, peças de reposição ou planos alternativos diante de eventos imprevistos.

7. **Achar que eventos incertos têm causas e efeitos conhecidos e lineares**—Pensamentos críticos e sistêmicos são necessários para ver efeitos e ameaças emergentes.[16]

Essas transgressões e as principais observações relacionadas revelam preconceitos executivos e pontos cegos. Reconhecer essas fraquezas pode ser desconfortável, mas é necessário aprofundar o pensamento crítico exigido para entender as incertezas, instabilidades e tensões que geram risco cibernético no ecossistema digital em que uma organização opera.

Esse entendimento capacita os executivos para implementar um tratamento mais maduro do risco cibernético que vai do conforto de padrões à geração e prática de exercícios do cenário e playbooks. O objetivo é permitir a uma organização manter uma postura vigilante diante da inevitabilidade de falha e exibir o devido cuidado e diligência no monitoramento e na garantir de riscos cibernéticos.[17]

Como Superar a Ilusão de Controle

Para encontrar formas concretas de superar a ilusão de controle, é necessário pensar no controle como a harmonia entre a limitação de instabilidades e a ampliação de incertezas. O objetivo é encontrar o nível correto de navegação vigilante em que a organização pode aprender e constantemente reconfigurar suas capacidades para responder a risco cibernético, mantendo as operações com o mínimo de efeitos adversos para entregar sua proposta de valor para os seus clientes.

Para fazer isso, é necessário visualizar a gestão de segurança cibernética a partir de um ponto de vista sistêmico-cibernético que implica manter um ciclo de garantia para o risco conhecido. As práticas e os padrões conhecidos permitem que uma organização mantenha operações em conformidade com requisitos básicos. Um ciclo adaptativo que incentiva suposições desafiadoras, gerando cenários de incertezas e ameaças emergentes e simulando eventos inesperados ajuda a criar uma capacidade para resiliência, permitindo que uma organização aprenda e desaprenda, e assim surpreenda seus adversários no seu próprio terreno conhecido, a incerteza.[18]

A encruzilhada desses dois ciclos está nos cenários, que criam oportunidade para a organização aprender. Nesses cenários, a organização declara o que não conhece e que está disposta a desenvolver toda a inteligência necessária para aprender com seu adversário e suas capacidades. Ela pode, então, voltar para o seu ciclo de garantia para identificar seus pontos cegos e buscar uma infraestrutura de configuração dinâmica capaz de ajustar-se às condições de mudança do ambiente.

> Uma organização terá controle de risco cibernético quando abraçar a incerteza e entender que ela é uma parte natural das operações e reconhecer e incorporar resiliência como parte da sua prática diária.

Essa contínua interação mantém a organização de pé e ciente de que está exposta a vulnerabilidades conhecidas e desconhecidas. Entender que a administração de segurança cibernética empresarial consiste em reduzir sua atratividade para invasores reduzindo as vulnerabilidades, aprender com os métodos dos invasores e resolver incidentes de segurança dentro dos limites da capacidade da organização é fundamental.[19] Consequentemente, a organização chega a um entendimento de que os exercícios de segurança e controle não resultam em ausência de falhas, vulnerabilidades e violações, mas na harmonia e no equilíbrio quando a inevitabilidade da falha é percebida. Isso cria uma oportunidade para aprender que desafia o conhecimento e a capacidade de inovação do adversário e da organização.

Assim, a organização terá controle do risco cibernético quando abraçar a incerteza e entender que isso é uma parte natural da operação e reconhecer e incorporar a resiliência como parte da sua prática diária. Há controle quando a segurança cibernética empresarial se traduz em um exercício de localização de limites e operação dentro do apetite de risco declarado pela organização. Esse tipo de controle pode deflagar os mecanismos de absorção e contenção diante de eventos incertos para manter as operações apesar de um evento adverso bem-sucedido.[20]

QUER SABER MAIS?

- Leia *Incorporating Risk Management into Agile Projects*. *www.isaca.org/incorporating-risk-management-into-agile-projects*
- Saiba mais, discuta e colabore com a gestão de riscos nos fóruns on-line da ISACA. *https://engage.isaca.org/onlineforums*

Próximos Passos

Quando os conselhos diretores têm conhecimento de que suas organizações operam e evoluem em ecossistemas digitais cruzados por risco cibernético, eles devem tomar medidas para tratar as sete transgressões das equipes executivas na administração desse risco, incluindo:[21]

- Identificar as partes responsáveis e as partes interessadas em segurança cibernética em cada área
- Identificar as circunstâncias específicas que aumentam o risco cibernético em cada área
- Criar um conselho de risco cibernético composto pelos responsáveis por risco cibernético em cada área, incluindo o diretor de segurança da informação e, no mínimo, um membro do conselho diretor, para ocupar as funções de:
  - Analisar as circunstâncias que aumentam o risco cibernético na área e determinar o apetite de risco.
  - Propor um plano de ação para administrar o risco cibernético
  - Apresentar o plano para a equipe executiva e o conselho diretor
  - Informar o progresso do plano para as partes interessadas
  - Avaliar os resultados do plano trimestralmente para relatórios para a equipe executiva e o conselho diretor

Conclusão

Administrar o risco cibernético nas organizações modernas é um desafio constante de aprender e desaprender. Exige superar seus próprios preconceitos sobre a gestão de risco tradicional e pensar na incerteza como um aliado para criar novas oportunidades e afinar os limites operacionais da organização quando as coisas não funcionam de acordo com o plano.[22] É um exercício que visa não proteger ou reduzir o risco, mas sim garantir a proposição de valor e fortalecer as capacidades comerciais diante da inevitabilidade de falha.

Controlar não é só limitar, mitigar e reduzir ataques, vulnerabilidades e falhas que são geralmente conhecidas. Essa abordagem se traduz em um ciclo de regulação e um ciclo de adaptação, que implica ampliar incertezas e instabilidades a partir do projeto e da simulação de cenários baseados em risco latente e emergente, que cria novas oportunidades de aprendizagem.[23] Quando isso é entendido, é possível superar a ilusão de controle tradicional baseado na inércia e na miopia associadas com as poucas certezas que podem ser mantidas, graças à aplicação de melhores práticas e à instalação e operação das ferramentas tecnológicas mais avançadas disponíveis.

A gestão de risco cibernético é dinâmica porque as condições sempre mudam, e o fluxo de informação é constante e geralmente inesperado.

Controle é um exercício baseado em dois ciclos: regulação e adaptação. Regulação ajuda a limitar, mitigar e reduzir ataques, vulnerabilidades e falhas, enquanto adaptação ajuda a ampliar incertezas e instabilidades dos cenários de simulação e projeto com base no risco latente e emergente para criar novas oportunidades de aprendizagem.[24] Com esse entendimento, é possível superar a ilusão de controle tradicional com base na inércia e na miopia associadas a poucas certezas que podem ser mantidas, graças à aplicação de melhores práticas e à instalação e operação das ferramentas tecnológicas mais avançadas disponíveis.

A gestão de risco cibernético é dinâmica porque as condições sempre mudam, e o fluxo de informação é constante e geralmente inesperado. Assim, isso exige um mudança de pensamento que estabeleça um novo paradigma para os profissionais de segurança e controle.[25] Implica reconhecer a organização como parte de um ecossistema digital em que é necessário saber como ela pode ser afetada por outros e como os outros podem ser afetados por ela. Consequentemente, não é apenas uma questão de garantir o que acontece interiormente, mas também aproveitar as oportunidades com outros parceiros estratégicos no ecossistema.

A gestão de risco cibernético envolve a configuração de uma empresa digital adaptável para permitir flexibilidade, autonomia, orquestração e descoberta de novas oportunidades nas bases da sua arquitetura corporativa (ou seja, modelo de negócios, operações comerciais, estratégia). Isso permite que a organização aproveite a instabilidade e a incertezas que as mudanças produzem, seja resiliente e entregue novas proposições de valor para os seus clientes.[26]

Notas finais

1 Subramaniam, M.; *The Future of Competitive Strategy: Unleashing the Power of Data and Digital Ecosystems*, MIT Press, USA, 2022

2 Capra, F.; *The Web of Life. A New Scientific Understanding of Living Systems*, Anchor, USA, 1997

3 Taleb, N.; D. Goldstein; M. Spitznagel; "The Six Mistakes

Executives Make in Risk Management," *HBR's 10 Must Reads on Managing Risk*, Harvard Business School Publishing, USA, 2020

4 Zeijlemaker, S.; M. Siegel; "Capturing the Dynamic Nature of Cyber Risk: Evidence From an Explorative Case Study," *Proceedings of the 56th Hawaii International Conference on System Sciences*, 27 December 2022, *https://hdl.handle.net/10125/103372*

5 André, C.; "Uncertainty Invites Wisdom," *Mind and Brain*, May/June 2021, *https://www.investigacionyciencia.es/revistas/mente-y-cerebro/la-presin-del-tiempo-833/la-incertidumbre-invita-a-la-sabidura-19848*

6 Meyer, R.; H. Kunreuther; *The Ostrich Paradox: Why We Underprapare for Disasters*, Wharton Digital Press, USA, 2017

7 Buheji, M.; D. Ahmed; H. Jahrami; "Living Uncertainty in the New Normal," *International Journal of Applied Psychology*, 13 August 2020, *http://article.sapub.org/10.5923.j.ijap.20201002.01.html*

8 Beer, S.; *Decision and Control: The Meaning of Operational Research and Management Cybernetics*, John Wiley and Sons, United Kingdom, 1994

9 Martinez-Moyano, I.; R. Oliva; D. Morrison; D. Sallach; "Modeling Adversarial Dynamics," *Institute of Electrical and Electronics Engineers 2015 Winter Simulation Conference (WSC)*, December 2015, *https://ieeexplore.ieee.org/document/7408352*

10 World Economic Forum, "Understanding Systemic Cyber Risk," Global Agenda Council on Risk and Resilience, October 2016, *https://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf*

11 European Systemic Risk Board, *Systemic Cyber Risk*, Germany, February 2020, *https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf*

12 Cano, J.; "Security Risk Management and Cybersecurity: From the Victim or From the Adversary?" *Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications*, 3 January 2023, *https://link.springer.com/chapter/10.1007/978-3-031-20160-8_1*

13 *Op cit* Zeijlemaker and Siegel

14 Deloach, J.; "The Top Risks for 2023: A Global View," NACD BoardTalk, 4 January 2023, *https://blog.nacdonline.org/posts/top-risks-2023-global*

15 Lam, J.; *Implementing Enterprise Risk Management. From Methods to Applications*, John Wiley and Sons, USA, 2017

16 *Op cit* Taleb *et al.*

17 Day, G.; P. Schoemaker; *See Soon, Act Faster: How Vigilant Leaders Thrive in an Era of Digital Turbulence*, MIT Press, USA, 2019

18 Cano, J.; "Rethinking the Practice of Security and Cybersecurity in Organizations: Systemic-Cybernetic Review," Global Strategy, Report No.58, 2020, *https://global-strategy.org/repensando-la-practica-de-la-seguridad-y-la-ciberseguridad-en-las-organizaciones-una-revision-sistemico-cibernetica/*

19 Zeijlemaker, S.; *Managing the Dynamic Nature of Cyber Security: A Future-Proof Strategy, This Is How It Works*, Disem Institute, Netherlands, 2022

20 Coden, M.; M. Reeves; K. Pearlson; S. Madnick; C. Berriman; "An Action Plan for Cyber Resilience," *Sloan Management Review*, 4 January 2023, *https://sloanreview.mit.edu/article/an-action-plan-for-cyber-resilience/*

21 Falco, G. *et al.*; "Cyber Crossroads: A Global Research Collaborative on Cyber Risk Governance", Cyber Crossroads, 2021, *https://arxiv.org/abs/2107.14065*

22 *Op cit* André

23 *Op cit* Cano, 2020

24 *Ibid.*

25 Medoh, C.; A. Telukdarie; "The Future of Cybersecurity: A System Dynamics Approach," *Procedia Computer Science, 3rd International Conference on Industry 4.0 and Smart Manufacturing*, 8 March 2022, *https://doi.org/10.1016/j.procs.2022.01.230*

26 Woerner, S., P. Weill; I. Sebastian; *Future Ready, The Four Pathways to Capturing Digital Value,* Harvard Business Review Press, USA, 2022