Recherche Maverick* : vous serez piraté, alors acceptez la violation

9 décembre 2022 - ID G00749245 - 23 minutes de lecture

Par **et 1 de plus** Michael Kelley , Katell Thielemann ,

Les failles de cybersécurité sont inévitables, mais de nombreux responsables de la sécurité et de la gestion des risques pensent encore qu'ils peuvent empêcher tous les piratages en jetant des personnes et de l'argent sur leurs défenses. Au lieu de s'efforcer de prévenir les violations, ils devraient se concentrer sur la résilience et considérer les piratages comme des incidents dont ils peuvent tirer des leçons.

Aperçu

Attention spécifique aux non-conformistes

Cette étude Maverick* contredit l'idée dominante selon laquelle les failles de cybersécurité peuvent être évitées et que les investissements destinés à les dissuader sont de l'argent bien dépensé. Cette croyance est manifestement fausse , car les violations se produisent encore souvent et à grande échelle. Dans la course aux armements qui s'intensifie, d'une part pour révéler et exploiter les vulnérabilités, et d'autre part pour les prévenir ou les dissimuler, les hackers , et notamment certains États-nations, sont gagnants. De plus, ils semblent détenir une avance inattaquable sur les programmes et pratiques de cybersécurité. Malgré cela, les organisations continuent d'affecter d'énormes ressources pour tenter de prévenir les violations – des investissements qui génèrent de faibles rendements et qui pourraient être réorientés pour créer une réelle valeur commerciale. Étant donné que cette recherche contredit les idées reçues, ses conclusions doivent être traitées avec prudence .

Résultats non-conformistes

- Les progrès de la cybersécurité continuent de se produire, même si les dépenses en matière de cybersécurité restent élevées et que les organisations de cybersécurité sont généralement bien financées et dotées d'un personnel complet. La conclusion incontournable est que les violations, qu'elles ciblent des organisations spécifiques ou qu'elles affectent des spectateurs innocents en général, ne peuvent être évitées.

- Les failles chez Maersk et Merck, les récentes attaques contre Colonial Pipeline et JBS, ainsi que les retombées de Stuxnet et des attaques SolarWinds et Kaseya, démontrent que les hacks

se sont déplacés vers les environnements opérationnels dans tous les secteurs. Ce faisant, ils ont étendu la menace du monde cybernétique au monde physique.
- Les organisations qui n'ont pas prévu l'échec aggraveront cette erreur en poursuivant une réponse « au fur et à mesure » aux cyberattaques. Pour faire une réelle différence dans l'impact des incidents de cybersécurité, les priorités en matière de cybersécurité doivent passer des stratégies défensives à la gestion des perturbations par la résilience.

Recommandations non-conformistes

Les responsables de la sécurité et de la gestion des risques doivent :

- Réduisez immédiatement les dépenses défensives en matière de cybersécurité et réorientez-les vers des initiatives de résilience.
- Apprenez de la théorie des accidents normaux (NAT) en appliquant les approches de « pleine conscience » des organisations hautement fiables (HRO) à la cybersécurité, afin de créer une organisation cyber-résiliente .
- Embauchez pour l'échec : employez des leaders en cybersécurité qui portent les cicatrices d'une vaste expérience en matière de violations – des guerriers de la cybersécurité aguerris qui comprennent comment atteindre la résilience .
- Faites de la cybersécurité un enjeu commercial en transformant les initiatives de cybersécurité grâce à une exposition à des disciplines telles que la reprise après sinistre et la continuité des activités .

Hypothèse de planification stratégique

D'ici 2025, les responsables de la sécurité et de la gestion des risques possédant une vaste expérience en matière de violations recevront une rémunération 30 % plus élevée que ceux qui n'en ont pas.

Recherche non-conformiste

Les recherches de Gartner Maverick* proposent des idées révolutionnaires, disruptives et parfois contradictoires qui remettent en question la pensée conventionnelle. Créé au sein de notre incubateur de recherche, il est conçu pour explorer des opportunités et des risques alternatifs qui pourraient influencer votre stratégie.

Analyse

Rien qu'en 2020, les 10 principales violations de cybersécurité ont exposé, selon une estimation prudente, plus de 30 milliards d'enregistrements, et les attaques de ransomwares se sont déplacées vers des environnements opérationnels dans tous les secteurs (voir **Les 10 principales violations de données de 2020**). Le paysage des menaces s'étend désormais bien au-delà du domaine de la sécurité des données , avec des attaques de ransomwares à la fois ciblées et percutantes. Ce n'est plus seulement le cybermonde qui est en danger. Le monde physique, y compris nos vies, nos systèmes de production et nos biens, est également en danger, comme le

montrent clairement les récentes attaques contre Colonial Pipeline et JBS, une grande entreprise de transformation de viande.

Même une faille de sécurité ou un exploit ciblé peut désormais avoir des impacts dévastateurs bien au-delà du foyer de l'attaque. Lorsque, par exemple, le logiciel malveillant NotPetya a été lancé pour cibler un logiciel de préparation de déclarations de revenus en Ukraine, de nombreuses entreprises lointaines, dont Maersk et Merck, ont subi des dommages collatéraux totalisant des milliards de dollars.

En outre, les attaques de la chaîne d'approvisionnement comme SolarWinds et Kaseya ont démontré la menace de vecteurs d'attaque totalement imprévus, que presque aucun outil de cybersécurité ne pouvait détecter ou atténuer.

> **La cybersécurité nécessite une nouvelle approche et une nouvelle réflexion en termes de stratégie.**

Dans son livre *Normal Accidents: Living With High-Risk Technologies* , le sociologue Charles Perrow a étudié des accidents majeurs comme l' explosion de la navette spatiale Challenger en 1986 et la catastrophe nucléaire de Tchernobyl la même année. Il est arrivé à la conclusion que certains systèmes comportent des risques qui ne peuvent être atténués par des moyens conventionnels. Sa définition de ces risques se résume à « des interactions complexes versus linéaires, et des couplages serrés versus lâches ». » Ses recherches ont révélé que, dans les organisations soumises aux risques associés à des interactions complexes et à des couplages étroits, les accidents sont inévitables : ils deviennent essentiellement « normaux », voire attendus.

Cependant, un ouvrage ultérieur, *Gérer l'inattendu : assurer des performances élevées à l'ère de la complexité,* des sociologues Karl E. Weick et Kathleen M. Sutcliffe , a étudié certaines de ces organisations complexes et est parvenu à des conclusions différentes. Les auteurs ont constaté que certaines organisations avaient développé une approche qui réduisait, voire éliminait, la possibilité d'accidents « normaux » ou leur impact sur l'organisation lorsqu'ils se produisaient.

Weick et Sutcliffe ont défini cinq traits de « pleine conscience » que l'on retrouve chez ce qu'ils définissent comme les HRO :

1. Sensibilité aux opérations
2. Réticence à simplifier à l'excès les raisons des problèmes
3. Préoccupation face à l'échec
4. Déférence envers l'expertise

5. Engagement envers la résilience

Leur étude a utilisé le terme « pleine conscience » de manière très délibérée pour désigner l'état d'être *toujours* conscient et attentif, de telle sorte que ces traits deviennent si répandus qu'ils deviennent presque automatiques.

En quoi les découvertes des sociologues sont-elles pertinentes pour la cybersécurité ? Presque tous les environnements technologiques actuels peuvent être définis comme impliquant des interactions complexes et comme étant étroitement couplés. Ainsi, même si Perrow étudiait les accidents, nous pensons que ses idées peuvent être appliquées à la cybersécurité.

Tout comme Perrow a défini les accidents comme inévitables dans des organisations très complexes et étroitement liées, il en va de même pour les violations de cybersécurité : elles sont « normales », attendues et inévitables. Cela signifie que l'objectif traditionnel de la cybersécurité – stopper les intrusions à tout prix – est tout simplement irréalisable et devrait être abandonné au profit de stratégies plus réalistes et plus efficaces. Ce changement est particulièrement urgent à mesure que les risques deviennent de nature cyber-physique.

Est-il possible d'organiser une pratique de cybersécurité autour de l'idée que les failles sont normales et attendues ? Plus important encore, peut-on bâtir une organisation de cybersécurité efficace dans laquelle cette idée est une conviction fondamentale, et qui protégera l'entreprise de l'impact des violations ?

> **Les organisations dotées de stratégies HRO ont réussi à réduire ou à éliminer les dommages commerciaux causés par les accidents. Pour la première fois, nous présentons un modèle dans lequel de telles stratégies peuvent être appliquées à la cybersécurité afin de réduire ou d'éliminer les dommages causés aux entreprises par des violations de cybersécurité.**

Organisations cyber-résilientes

Une organisation cyber-résiliente (CRO) est une organisation dans laquelle l'accent mis sur la cybersécurité a peu à voir avec les mesures et stratégies traditionnelles et beaucoup à voir avec la prévention des dommages commerciaux (par-dessus tout) au moyen d'une stratégie de résilience et de reprise. Tout comme les HRO peuvent continuer à exercer leurs activités malgré les « accidents normaux », les processus commerciaux des CRO peuvent se poursuivre malgré les perturbations de la cybersécurité.

En modifiant légèrement la définition de la « pleine conscience » adoptée par Weick et Sutcliffe pour les HRO, nous avons défini les cinq traits clés des CRO.

La figure 1 montre les cinq traits des HRO identifiés par Weick et Sutcliffe. La figure 2 identifie les cinq caractéristiques des CRO, telles qu'identifiées par Gartner. Le tableau 1 mappe ensuite les caractéristiques des HRO à celles des CRO.

Figure 1 : Les cinq caractéristiques des organisations hautement fiables

Figure 2 : Les cinq caractéristiques des organisations cyber-résilientes

The Five Traits of Cyber-Resilient Organizations (CROs)

Source: Gartner
749245_C

Gartner

Tableau 1 : Traits HRO mappés aux traits CRO

Caractéristiques des organisations hautement fiables ↓	↓	*Caractéristiques des organisations cyber-résilientes* ↓
Sensibilité aux opérations	=	Ciblage de la cybersécurité minimale viable (MVC)
Une sensibilité aux opérations définit la manière dont un HRO s'efforce de garantir que tous les membres de l'organisation se concentrent sur la résilience. Cela correspond au trait CRO de définition, de mesure et de suivi de MVC. La définition et la maintenance de MVC nécessitent l'établissement d'une base minimale de cybersécurité qui permet à l'organisation de se concentrer sur la minimisation ou l'élimination de l'impact commercial des incidents de cybersécurité.		
Réticence à simplifier à l'excès les raisons des problèmes	=	Création et suivi d'un indice de cyber-résilience

Caractéristiques des organisations hautement fiables		*Caractéristiques des organisations cyber-résilientes*
Sa réticence à simplifier à l'excès les raisons des problèmes aide un HRO à creuser suffisamment profondément pour découvrir les causes profondes. Ce trait correspond au trait CRO de création (définition), de maintien et de suivi des progrès par rapport à un indice de cyber-résilience. Cela garantit que l'organisation peut découvrir et définir des mesures de base pour assurer la résilience, ce qui implique de trouver le bon équilibre entre la cybersécurité et la cyber-résilience.		
Préoccupation face à l'échec	**=**	**Transformer la cybersécurité en cyber-résilience**
La préoccupation d'un HRO face à l'échec l'encourage à devenir une organisation qui analyse constamment les événements et l'aide ainsi à réduire ou à prévenir les dommages commerciaux dus aux accidents. Cette caractéristique correspond à la caractéristique CRO de transformer la cybersécurité en cyber-résilience en donnant la priorité aux disciplines de reprise après sinistre et de continuité des activités par rapport à la discipline traditionnelle de la défense en matière de cybersécurité.		
Déférence envers l'expertise	**=**	**Embaucher pour l'échec**
Le respect de l'expertise encourage ceux qui possèdent des connaissances pertinentes à les apporter afin de prévenir ou de limiter les perturbations des activités, quelle que soit leur position. Ce trait HRO correspond au trait CRO d'embauche en cas d'échec, ce qui garantit que les dirigeants qui ont tiré les leçons de l'expérience des violations sont dans les bonnes positions pour réduire ou éliminer l'impact des incidents.		
Engagement envers la résilience	**=**	**Formation pour la reprise d'entreprise**
Un engagement en faveur de la résilience incite les dirigeants de HRO à poursuivre sans relâche leurs efforts pour éliminer l'impact commercial des accidents. Cette caractéristique correspond à la caractéristique CRO de formation à la reprise d'entreprise – plus précisément, la recherche résolue d'une résilience accrue afin d'éviter ou d'atténuer les impacts commerciaux des incidents de cybersécurité.		

Source : Gartner

Les cinq caractéristiques des CRO

Trait n°1 : Ciblage d'une cybersécurité minimale viable

La pratique du piratage informatique est en grande partie opportuniste, semblable à celle d'un voleur de voiture marchant dans une rue bordée de véhicules pour la plupart verrouillés à la recherche d'un véhicule non verrouillé. Par conséquent, laisser une organisation exposée aux pirates informatiques en n'appliquant pas de bonnes pratiques de cybersécurité est à juste titre considéré comme une négligence par les responsables de la cybersécurité.

Ainsi, même si nous pensons que la résilience doit avoir la priorité sur la défense, les pratiques standard de cybersécurité doivent toujours s'appliquer. Il reste essentiel de maintenir une sécurité bien conçue pour les réseaux d'entreprise et de préserver des pratiques de gestion des identités et des accès bien conçues, basées sur le principe du moindre privilège et de l'accès approprié. Il restera nécessaire de maintenir une visibilité sur toutes les transactions informatiques dans l'ensemble d'une organisation, et d'appliquer de bonnes pratiques d'hygiène de cybersécurité aux données, afin d'en garantir le chiffrement et les accès appropriés. De nombreuses publications Gartner peuvent vous aider à garantir que la visibilité est activée et que des contrôles sont en place pour toutes les menaces de cybersécurité standard et comprises.

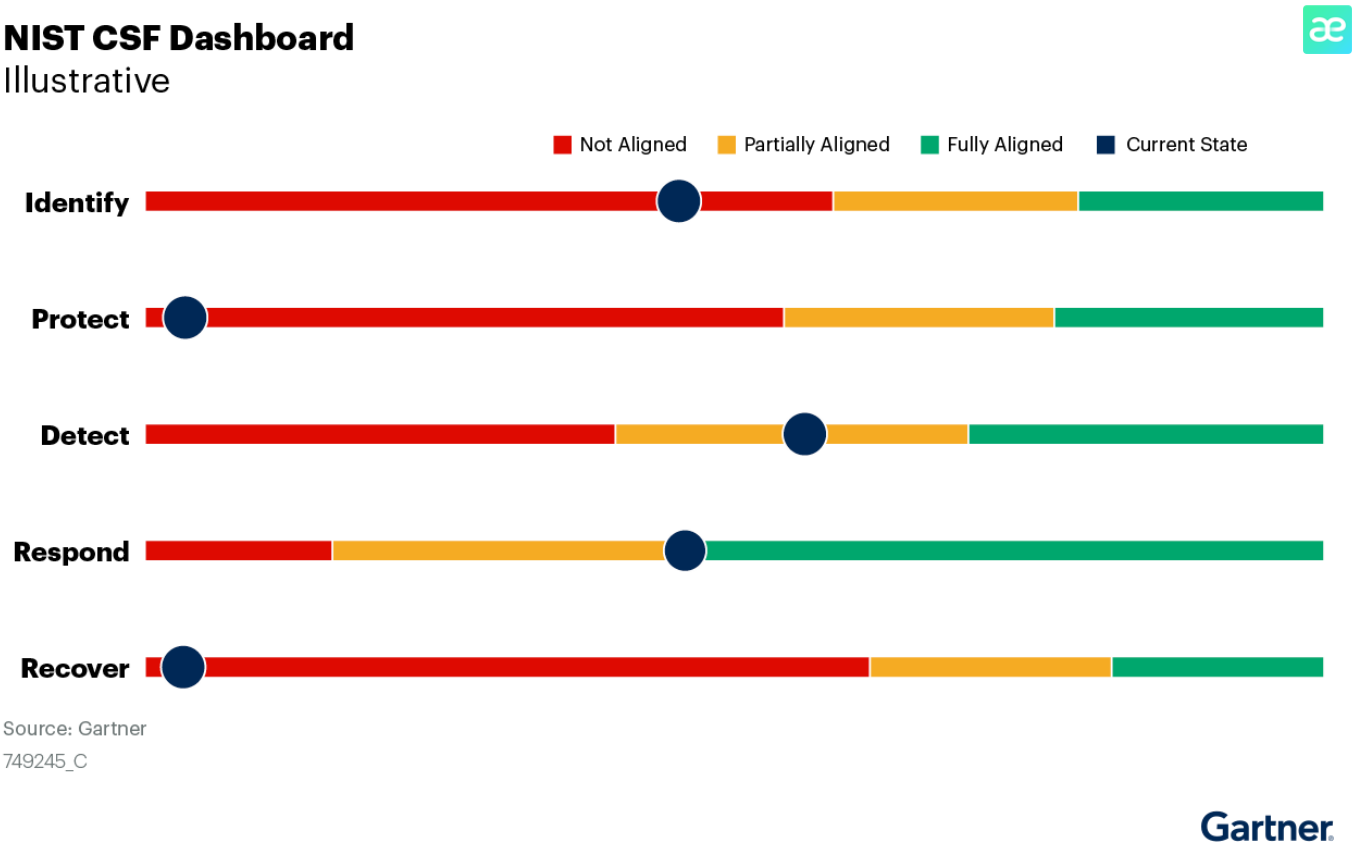
Le Gartner IT Scorecard est un bon moyen de comparer la situation de votre organisation en termes d'atteinte d'une cybersécurité minimale viable (MVC). L'adoption d'un modèle tel que le NIST Cybersecurity Framework (CSF) peut aider votre organisation à atteindre le MVC. La figure 3 montre un tableau de bord NIST CSF de base que vous pouvez utiliser.

Au-delà de la valeur de cybersécurité de l'identification et de la maintenance de MVC se trouve la valeur beaucoup plus importante de l'identification des coûts d'opportunité – en d'autres termes, des domaines de dépenses excessives en logiciels de cybersécurité.

> **Tout investissement dans des logiciels ou des ressources humaines au-delà des exigences de MVC doit être immédiatement réduit et réorienté pour améliorer la résilience.**

C'est dans ces domaines que se trouveront les opportunités de dépenses en faveur de la cyber-résilience. Les investissements dans la cybersécurité défensive au-delà de ce qui est nécessaire pour MVC représentent des coûts d'opportunité. Ces investissements peuvent être classés comme des investissements sous-performants axés sur des efforts défensifs, qui ne pourront jamais empêcher tout préjudice commercial. Il est préférable d'investir dans des stratégies visant à réduire ou éliminer l'impact commercial des failles de sécurité. Cela signifie investir dans la cyber-résilience.

Figure 3 : Exemple de tableau de bord du cadre de cybersécurité du NIST



Trait n°2 : Création et suivi d'un indice de cyber-résilience

La création et le suivi d'un indice de cyber-résilience seront essentiels pour déterminer le bon équilibre entre les dépenses consacrées au MVC et à la résilience. Mais cet indice et ses mesures paraîtront inhabituels du point de vue traditionnel de la cybersécurité. Par exemple, le temps entre les échecs (brèches) sera mesuré en fonction des opportunités de pratique et d'expérience. Fondamentalement, *plus le temps s'écoule entre les violations, moins l'organisation sera préparée et plus le score de résilience sera faible* . À l'inverse, plus les violations se produisent fréquemment, plus l'équipe de cybersécurité s'entraînera et sera mieux préparée à réagir et à prévenir ou atténuer l'impact des violations futures.

Les mesures traditionnelles de cybersécurité, telles que la fréquence à laquelle les serveurs sont corrigés ou le nombre de tentatives d'intrusion, doivent être minimisées et la priorité doit être accordée aux mesures qui mesurent l'impact commercial des événements de sécurité. Un accent particulier doit être mis sur la mesure dans laquelle l'impact sur l'entreprise est réduit par les mesures de résilience mises en place grâce à l'expérience de l'équipe de cybersécurité dans la réponse aux failles de sécurité fréquentes, normales et attendues.

En vous concentrant sur la défense et l'évitement, votre organisation de cybersécurité ressemblera à un athlète ayant dépassé son apogée et essayant de rivaliser avec des athlètes jeunes, en forme et énergiques.

Si aucune violation ne s'est produite depuis trois ans ou plus, votre équipe de cybersécurité sera *moins préparée* à une future violation, et cette situation peut indiquer des dépenses excessives en contrôles défensifs de cybersécurité. Cette mesure sera différente pour chaque organisation. Votre organisation pourrait constater, par exemple, que son investissement dans des contrôles défensifs pour MVC entraîne une réduction de 99 % des violations de cybersécurité, mais que des dépenses supplémentaires dans les contrôles MVC pour réduire les violations de 99,9 % réduiraient sa cyber-résilience telle que mesurée par le cyber-résilience. -indice de résilience. Ce dépassement défensif signifierait que lorsque de futures violations se produiraient – et elles se produiraient – votre organisation serait moins en mesure de prévenir tout dommage pour l'entreprise.

Conversely, overspending on resilience initiatives to the detriment of MVC can also increase the risk of business disruption. You therefore need to strike a balance. On the one hand, you must spend only what is required to enable your definition of defensive MVC. On the other, you must spend more than you do on MVC to improve your organization's resilience.

Figure 4 illustrates the danger of overspending on either defensive security tools or resilience.

Figure 4: Balance Spending on Defense and Resilience to Reduce the Risk of Business Disruption

Source: Gartner
749245_C

Gartner

The time between cybersecurity breaches should be one component of your cyber-resilience index. Additional metrics may relate to:

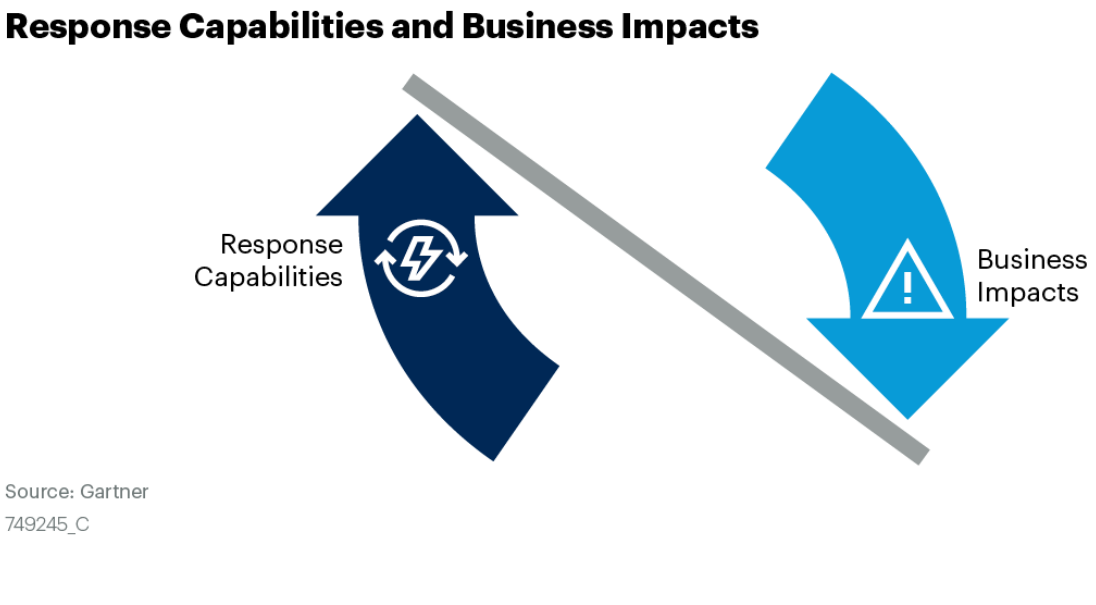
- The establishment and maintenance of MVC
- General staff experience with breaches
- The experience of key cybersecurity leaders

- The maturity of process definition
- The frequency of exercising the computer security incident response team and business resumption/downtime procedures.

Note that artificial exposure to breaches is insufficient for an organization to get the practice it needs to deal with future breaches. You may be tempted simply to allow a few “script kiddies” access to your systems as part of a breach exercise. But this would not build the capability you need to cope with a significant breach. It would be analogous to a would-be weightlifter lifting one-pound weights — the challenge would be insufficient to build enough “resilience muscle memory” (RMM) to improve your organization’s position on the cyber-resilience index. In any case, given that actual breaches are normal and expected, artificial exercises are unnecessary.

As Figure 5 shows, the way to reduce the business impact of a breach is to increase response capabilities, particularly your organization’s RMM. Building response capabilities enables an organization to act faster, make wiser decisions, allocate resources more effectively and manage communications better. In essence, like a sportsperson entering an event, you do much better if you have trained in advance (see Note 2 for a supply-chain-specific example).

Figure 5: Increasing Response Capabilities Reduces Business Impacts



Trait No. 3: Transforming of Cybersecurity Into Cyber-Resilience

We have established that breaches are normal in highly complex and tightly coupled organizations, and that the key to minimizing business damage is to develop resilience. The science of NAT and HROs is embedded in the disciplines of business continuity and disaster recovery. These disciplines are certainly about working to prevent business disruption, but they go further than defensive cybersecurity approaches by defining, planning and practicing responses to events, such as cybersecurity breaches, that interrupt business.

Transforming cybersecurity into cyber-resilience involves prioritizing resilience over defense, and elevating the native disciplines and skills used by the business continuity management office above cybersecurity teams' traditionally defensive strategies.

Whether the cybersecurity team is merged with the business continuity management (BCM) office, or the BCM office is given oversight of cybersecurity, a strategy for achieving the right level of discipline for resilience, response, recovery and restoration is essential. Such a strategy will enable recovery disciplines to be applied more effectively in order to minimize the impact of breaches. It requires an acceptance that cybersecurity breaches will occur and that they will give cybersecurity leaders the opportunity to practice their plans prior to further breaches.

When the global pharmaceutical organization Merck was hit by NotPetya in the same attack that crippled the logistics company Maersk, Merck was more severely impacted because it applied crisis management practices to its physical assets, but not its cybersecurity assets. Consequently, it wasted time arguing about whether the event was a crisis from an IT perspective. The disciplines of resilience and recovery must be applied equally across the physical and cyber domains in order to mitigate business risk.

If your organization has not already promoted the head of the office of resilience — or more likely, of the BCM program office — to a C-level position, this is a good time to do so. We recommend appointing a "chief resilience officer" responsible for business impacts from both a physical and a cybersecurity perspective.

The goal of transforming cybersecurity into cyber-resilience is to create a culture of resilience. Although proving the efficacy or ROI of security awareness training is difficult, it was a person questioning the validity of a request for multifactor authentication who revealed elements of the SolarWinds hack in one organization. This kind of questioning must become part of your culture, so that every person is willing, without fear of reprisal, to report anomalies to a crisis management group.

Trait No. 4: Hiring for Failure

CIOs and CISOs are hired to defend their business and construct a cybersecurity capability that prevents all intrusions, all breaches. And when they fail to do so — as they will — they often become scapegoats (see 7 Security Incidents That Cost CISOs Their Jobs). New cybersecurity leaders are then brought in, typically ones who can say they have never experienced a breach. But given the inevitability of cybersecurity incidents, this lack of experience is attributable less to their cybersecurity skills than to their luck (so far). This approach is analogous to hiring a trial lawyer who has never been inside a courtroom and expecting them to win their first case, or putting a promising high-school baseball player on a professional team and expecting them to succeed.

After a breach, the value of a cybersecurity leader actually becomes *higher*, not lower, because that experience, and the associated trial-and-error mitigation exercises, contribute to his or her RMM. Rather as repeated lifting of weights increases a person's physical strength, so repeated exposure and response to breaches *increases* a cybersecurity leader's ability to think and plan for resilience — and, most importantly, to mitigate damage to the business.

> **The importance of prior exposure to breaches should prompt a complete shift in how you think about hiring and retaining cybersecurity leaders.**

It follows that some of the most valuable cybersecurity leaders are those who have experienced cybersecurity breaches, potentially even highly visible hacks, because they have had to develop plans to mitigate the resulting business damage — because they have RMM. From this perspective, firing a cybersecurity leader because of a breach robs the organization of the very person it needs to build resilience (unless the breach occurred as a result of that person's incompetence or failure to implement MVC cybersecurity practices).

Businesses should hire cybersecurity leaders who *have* experienced breaches, even highly public breaches. Through that experience, in which, by trial and error, they would have discovered what succeeded and what failed, they would have learned how to reduce the resulting business damage, or even prevent any. In other words, "hiring for failure" is about hiring people who bear the scars of battle and have enough RMM to help your business avoid business damage from future cybersecurity incidents.

Trait No. 5: Training for Enterprise Recovery

The key to diverting money from defense and prevention to resilience is to develop a discipline around recoverability.

An old military maxim says that "No plan of operations extends with certainty beyond the first encounter with the enemy's main strength." Similarly, U.S. President Dwight Eisenhower said that "the very definition of 'emergency' is that it is unexpected; therefore, it is not going to happen in the way you are planning" (see **Strategic Planning: Moltke the Elder, Dwight Eisenhower, Winston Churchill, and Just a Little Mike Tyson**). These insights underline the importance of embracing cybersecurity breaches, so that cybersecurity teams get plenty of practice of dealing with new types of attack, new attack strategies and means of recovery.

> **Cybersecurity incidents should be embraced, because they give you the real-world opportunity to experience the randomness of cybersecurity attacks and to fine-tune your response and recovery plans.**

Two concepts associated with NAT and HROs further demonstrate the need for training in order to help ensure an enterprise's recovery.

The first is *practical drift*. When an organization "drifts away" from established practices for the sake of convenience, this represents a failure of vigilance. Practical drift reduces an organization's resilience and RMM (see Figure 6). Practice in how to avoid it is therefore important.

Figure 6: Practical Drift Reduces Resilience

The second is *normalization of deviance*, which you must also practice to avoid, as far as possible. This is where something out of the ordinary occurs day after day, but nobody sees any associated problem. So, although the occurrence is abnormal by definition, no one pays attention to it. It has, in essence, become "normal." The problem with this is that, in the world of cybersecurity, a deviation that triggers only what could be described as a "yellow blinking light" can indicate a larger and more serious problem (see Figure 7). It may, for example, point to an advanced persistent attack that no other monitor or control is picking up.

Figure 7: The Normalization of Deviance — a Yellow Blinking Light

Normalization of Deviance

Source: Gartner
749245_C

Gartner

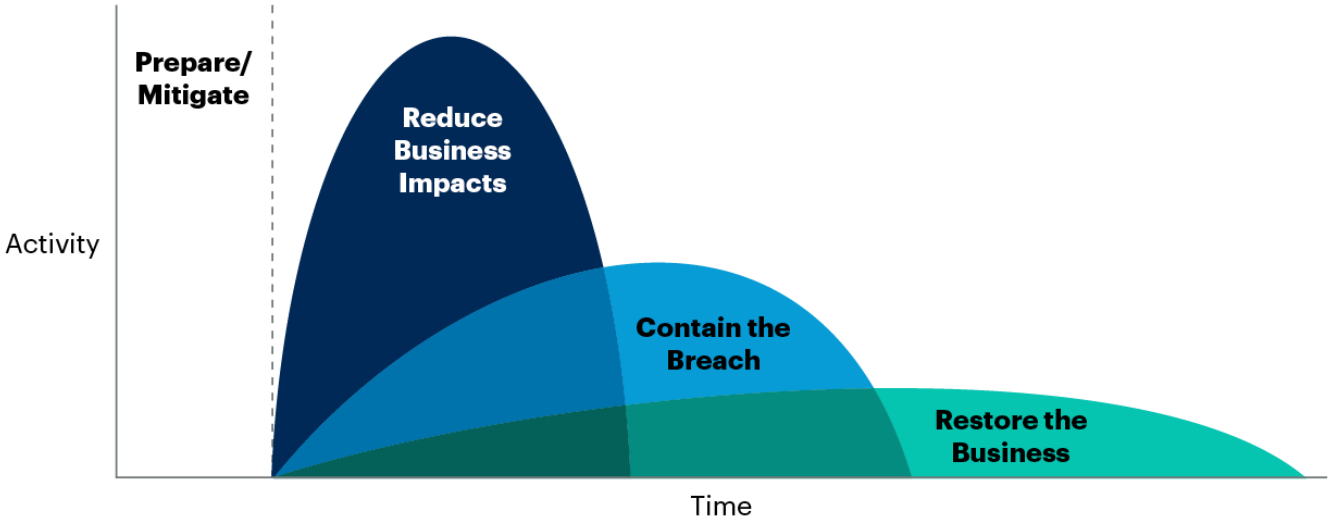
A consideration with regard to penetration testing is that although such testing serves a useful role in training and building RMM, it is, by itself, inadequate preparation for a breach. Penetration testing involves a degree of predictability that, on its own, will not enable leaders to build up enough RMM to help them be effective when it matters. Unscripted attacks that only the CISO knows about can help, but the key thing is for leaders, including the CISO, to have the opportunity to experience and respond to the *randomness* of cybersecurity attacks.

Another consideration is that when a cybersecurity breach occurs, the affected organization's ability to provide goods and services to its end users must be protected. The ability to manage any disruption effectively is essential to prevent long-term damage to an organization's financial, legal and reputational standing. This means that the responding personnel have a collective responsibility. Everyone must work together in response to a cybersecurity breach, as this will give the organization the best chance of prevailing.

It is of utmost importance to reduce or eliminate business impacts, to ensure that the business is unaffected by what is going on in terms of cybersecurity. Secondarily, the breach must be contained. And, thirdly, work must be done to restore the business (see Figure 8).

Figure 8: CRO Response Phases

CRO Response Phases



Source: Gartner
749245_C

Gartner

Conclusion

Cybersecurity breaches are inevitable and unavoidable, however many resources you allocate to prevent them. This reality reveals two problems with current cybersecurity practice:

- Current cybersecurity strategies, which focus on defense, are inadequate to prevent business disruption.
- Cybersecurity leaders treat cybersecurity incidents as events to be avoided at all costs, which is an impossibility.

In this Maverick research we have argued that cybersecurity leaders must instead divert resources from defense to resilience and treat breaches as opportunities from which to learn how to be more resilient in future.

> **Focusing exclusively on defensive cybersecurity hurts an organization's ability to develop sound resilience strategies to reduce, or even eliminate, the business impact of security incidents.**

More specifically, the correct strategy is to develop RMM through repeated exercises, to refine your resilience and recovery ability, and ultimately ensure that breaches are minor hiccups that do

not harm your business. The five traits of CROs described in this research are the keys to long-term mitigation of business damage from unavoidable cybersecurity breaches.

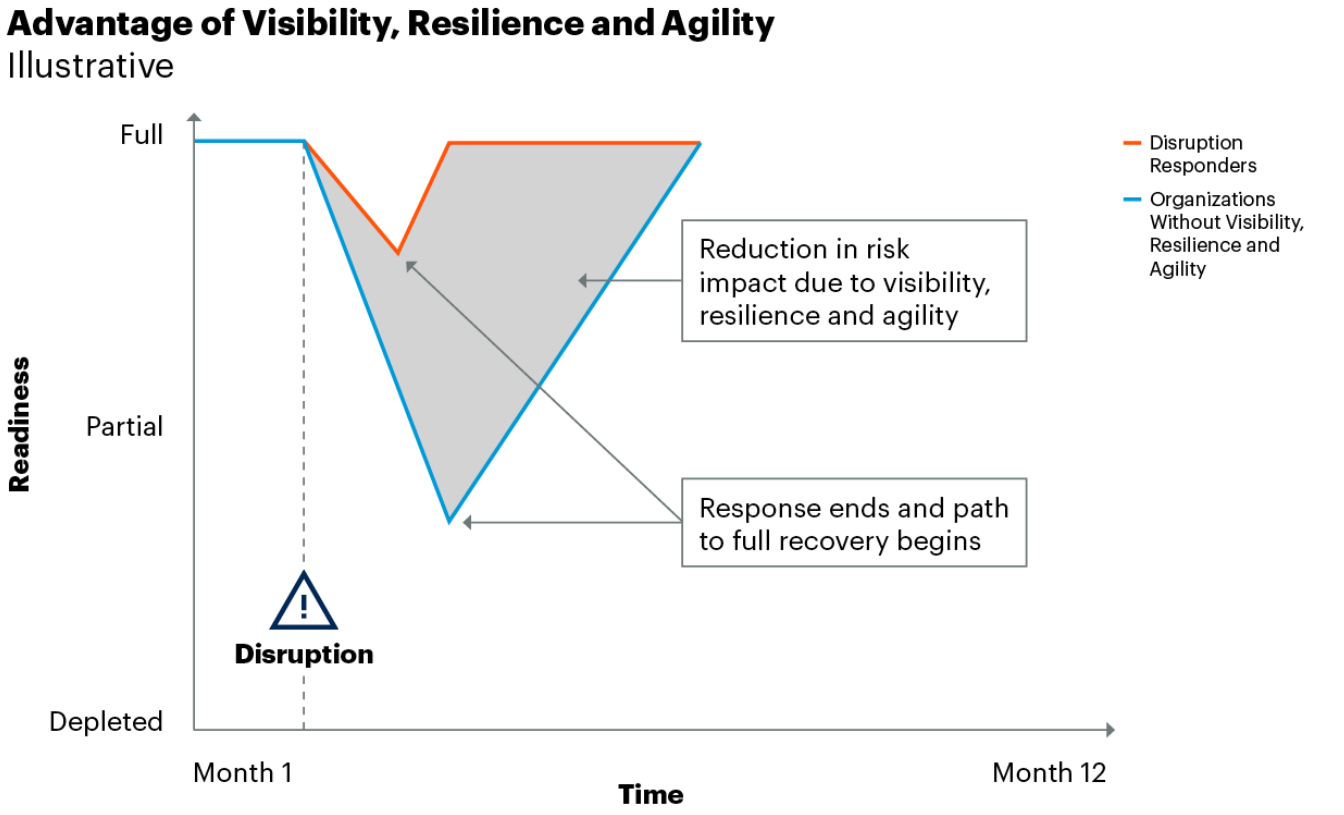
Evidence

- Gartner's **IT Key Metrics Data 2021: IT Security Measures — Analysis**
- Lucian Constantin , **L'attaque SolarWinds expliquée : et pourquoi elle était si difficile à détecter** , IDG Communications, 15 décembre 2020
- Charles Perrow, *Accidents normaux : vivre avec des technologies à haut risque* , rév. éd., Princeton University Press, 1999
- Karl E. Weick et Kathleen M. Sutcliffe, *Gérer l'inattendu : une performance résiliente à l'ère de l'incertitude* , Wiley, 2011
- Derek E. Bambauer, **Ghost in the Network** , *University of Pennsylvania Law Review* 162 (2014), 1011-91
- Samir Shrivastava et Frederica Pazzagila, **Théorie des accidents normaux versus théorie de la haute fiabilité : une résolution et un appel pour une vision des accidents par systèmes ouverts,** *Human Relations* 62 (2009), 1357-90
- Marc Goodman, *Crimes futurs : tout est lié, tout le monde est vulnérable et ce que nous pouvons faire pour y remédier* , Doubleday Books, 2015.
- Torgeir K. Haavik et autres, **HRO et RE : une perspective pragmatique** , *Safety Science* 117 (2019), 479-89
- Michael Hill, **#GartnerSEC : Adam Banks de Maersk réfléchit à la réponse et au rétablissement de NotPetya** , *Infosecurity Magazine* , 10 septembre 2019
- Rae Ritchie, **Maersk : Se remettre d'une cyber-attaque catastrophique** , Fujitsu, août 2019
- Joe Tidy, **Colonial Hack : Comment les cyberattaquants ont-ils coupé le pipeline ?** , BBC News, 10 mai 2021
- Rob McLean, Alexis Benveniste et Allie Malloy, **le principal producteur de viande JBS USA touché par une cyberattaque, probablement en provenance de Russie** , CNN Business, 2 juin 2021
- Dan Swinhoe, **7 incidents de sécurité qui coûtent leur travail aux RSSI** , IDG Communications, 2 janvier 2020
- Matt O'Brien, **Une attaque de ransomware avant les vacances laisse les entreprises se démener** , AP News, 3 juillet 2021

Note 2 : Façonner la perturbation pour réduire le temps de récupération

La figure 9 est extraite du document Shaping Disruption: A New Strategy for Supply Chain Risk Management de Gartner , qui définit un concept étroitement lié. Il montre qu'en appliquant le principe selon lequel les organisations doivent « façonner les perturbations », elles peuvent réduire considérablement le temps nécessaire à leur rétablissement. Cela démontre également que la planification de la résilience et de la reprise réduit considérablement les perturbations des activités. La présente recherche Maverick* démontre que la même idée peut être appliquée à la cybersécurité.

Figure 9 : La stratégie de réponse aux perturbations réduit l'impact



Source: Gartner
Note: A disruption is an unfamiliar risk event that actually impacts your organization.
747340_C

Gartner

© 2023 Gartner, Inc. et/ou ses sociétés affiliées. Tous droits réservés.