Top Security and Risk Management Trends

Published: 26 April 2018 **ID:** G00337028

Analyst(s): Peter Firstbrook, Earl Perkins, Jeffrey Wheatman, David Mahdi, Jie Zhang, Sam Olyaei

Senior executives are increasingly conscious of the impact cybersecurity can have on business outcomes. This attention provides a source of support for security and risk management leaders to take advantage of emerging trends to improve resilience and elevate their standing in the organization.

Key Trends

- Senior business executives are finally aware that cybersecurity has a significant impact on the ability to achieve business goals and protect corporate reputation.
- Legal and regulatory mandates on data protection practices are impacting digital business plans and demanding increased emphasis on data liabilities.
- Security products are rapidly exploiting cloud delivery to provide more agile solutions.
- Machine learning is providing value in simple security tasks and elevating suspicious events for human analysis.
- Security-buying decisions are increasingly based on geopolitical factors, along with traditional buying considerations.
- Dangerous concentrations of digital power are driving decentralization efforts at several levels in the ecosystem.

Recommendations

Security and risk management leaders seeking to capitalize on these trends should:

- Build a security program that can link security strategy with business initiatives.
- Ensure that digital business plans include both data protection costs and data liability considerations.
- Exploit the emerging cloud security services providers to improve security and reduce administration overhead.

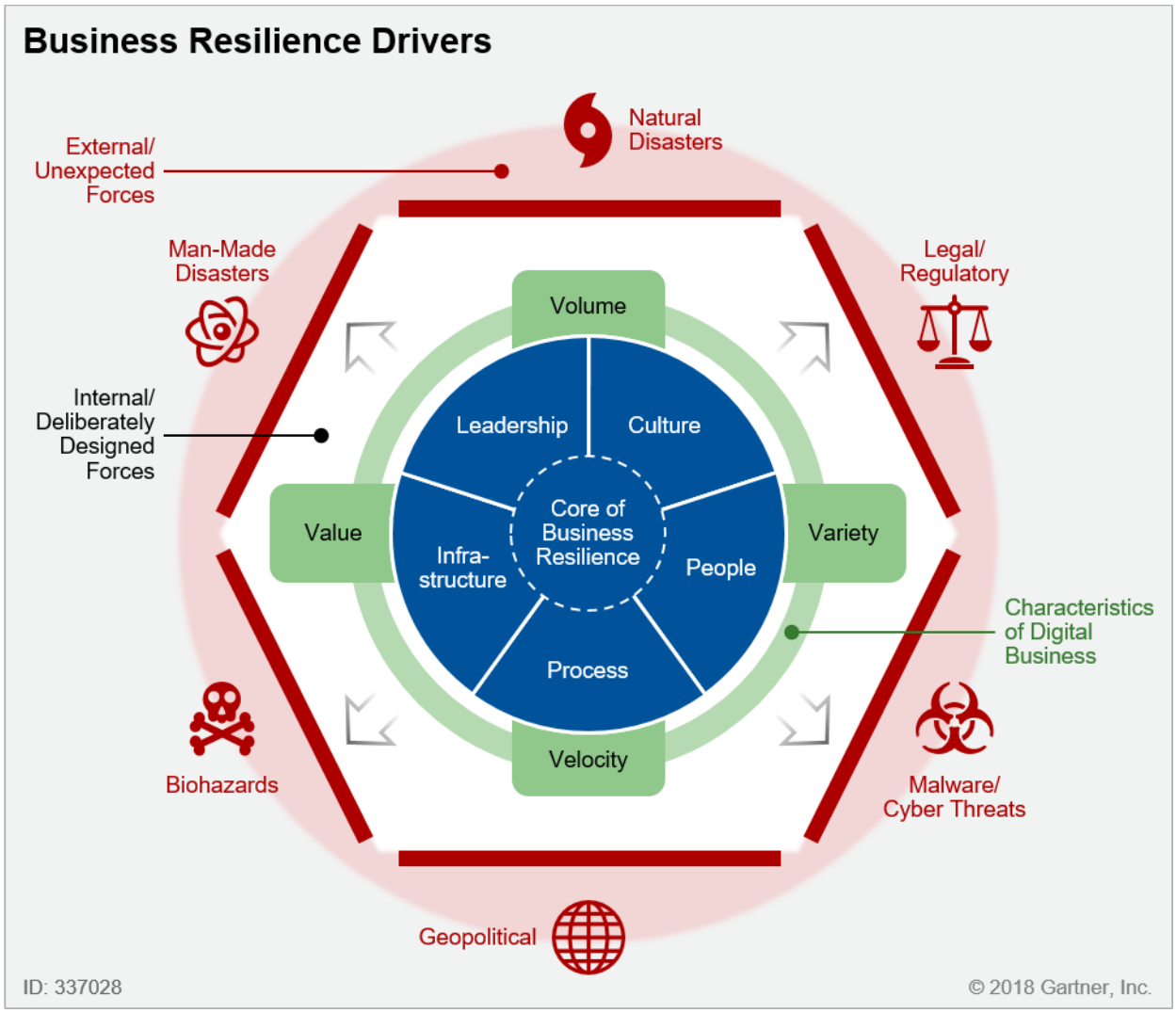
- Seek solutions that leverage machine learning but look for proof of value over other approaches.
- Ensure that digital business projects take into account the emerging geopolitical cyber landscape and concentration of digital resources.

Analysis

As we explore these trends in detail, it is important to point out the definition Gartner uses to identify top cybersecurity trends. In Gartner's definition, "top" trends highlight ongoing strategic shifts in the security ecosystem that aren't yet widely recognized, but are expected to have broad industry impact and significant potential for disruption. Through 2022, technologies and strategies related to these trends will reach a level of maturity that offers leaders valuable capabilities in the effort to secure digital business. This analysis does not predict what will happen. Rather, we aim to describe what's significant about what we see happening in the cybersecurity discipline.

The major triggers driving these trends include shifts in attacker tactics, new legal, regulatory and consumer expectations, and the increasing digitalization of all aspects of business and society. Together, these trends tell a broader story of the evolution and adaptation that cybersecurity must undergo in terms of technology, process, mindset and culture. Taking advantage of these trends will help organizations achieve two key strategic goals, business resilience (see Figure 1) and digital dexterity.

Figure 1. Business Resilience Drivers



Source: Gartner (April 2018)

Executives are increasingly aware of the impact security and data regulations can have on the costs and potential liabilities of digital business plans. However, security and risk management (SRM) leaders must evolve their organizations to take advantage of this new executive attention. The rapid expanse of cloud computing and software as a service (SaaS) is finally reaching the security products industry to help solve the skills shortage and to deliver more agile products. Concurrently, the shifting focus of security to detection and response, and to adaptive authentication, has created a mountain of data that can be mined using rapidly advancing machine learning (ML) tools to spot attackers and upskill operators. Meanwhile, the internet, which in its utopian infancy

was supposed to deliver decentralization and democratization, is starting to demonstrate dangerous levels of centralization of power, inspiring emerging efforts to find new technologies that can reverse this trend (such as blockchain). In the midst of all this, there is an escalating geopolitical cyberwar — often unseen but glaringly evident in election influence campaigns, infrastructure disruptions and data breaches — that could cause collateral damage to unwitting enterprise organizations.

Trends

Trend No. 1: Senior Business Executives Are Finally Aware That Cybersecurity Has a Significant Impact on the Ability to Achieve Business Goals and Protect the Corporate Reputation

Gartner has been saying for the past 10 years that security is a board-level topic (see Note 1), and a mandatory element of a clearly articulated digital business strategy. Business leaders were not necessarily receptive to that message. However, a string of recent high-profile incidents were so jarring that business professionals couldn't help but recognize how the hostility and aggression of technological crime could impact their business goals or even their job security.

Consider just a few of the recent headlines:

- Verizon received a $350 million discount on their purchase of Yahoo! as a result of Yahoo!'s data breach, which resulted in a failure to hit the standard of due care.
- Maersk took a $300 million expense as a result of a massive ransomware attack.
- Equifax's breach cost the CEO, CIO, and the CSO their jobs, and will have a continuing significant financial impact.
- Global economic losses from the "WannaCry" attack was estimated to be between $1.5 and $4 billion.

Business leaders and senior stakeholders now appreciate security as much more than tactical, technical stuff done by overly serious, unsmiling types in the company basement. However, security and risk management leaders still face numerous challenges in responding to attention from boards and executives. The good news is we have their attention. The bad news is we continue to speak a different language. As a result, security and risk management leaders lack a clear mandate from the business, and both groups are struggling with the ever rising complexity of digital business.

To capitalize on this trend, mature security organizations are investing in security and risk managers that have the background and experience to work closely with business stakeholders to understand

their risk appetite and risk tolerance. These organizations recognize that the role of security is not to protect the business from itself. Rather, it is to ensure the business knows what risks it faces and has enough information to make the best decisions about how much risk it will be willing to accept. These SRM leaders articulate all cybersecurity risks within the context of business objectives. In other words: "We need to do <this> at <this> level or the business will see <this> impact." Speaking the language of the business enables the business leaders to respond with a clearer security strategy mandate to guide the security organization.

Leading organizations are actively developing better board/executive and security partnerships. Board members are being educated on cybersecurity. Cybersecurity experts are being granted board membership. Independent parties are being invited to question CISOs in board meetings. Concurrently, these security organizations are acting more like the business. They are treating security as a business function, providing stakeholders with service levels that align with business risk, and showing clear cost optimization activities. These leading security organizations are setting goals and being held accountable by their boards.

Smart security organizations are not exploiting the board-level attention to simply go shopping for new security products. Instead, they are using this attention to gain executive-level sponsorship for new strategies to address the security skills shortage, by:

- Developing more virtual roles (such as virtual CISOs or privacy officers)
- Outsourcing more operational functions to MSSPs/MDRs
- Favoring cloud delivery products to reduce the maintenance overhead and stay current
- Increasing the level of automated operational functions
- Collaborating with universities, the military and other communities to attract emerging workers
- Implementing an inclusive workplace culture and recruitment practices to attract a more diverse talent pool
- Using lean security organization principles to drive security responsibilities more into the business and elsewhere in IT

Business leaders now understand the significant impact of security on an organization's ability to achieve business goals, protect the business and reputation, defend from the inevitable, and get back to full functionality. Security and risk managers will have to step up their game and create security programs that can interact with the business if they want to take advantage of the opportunity offered by this change of perception.

Recommendations:

To take advantage of newfound business support for security initiatives, security and risk management leaders should:

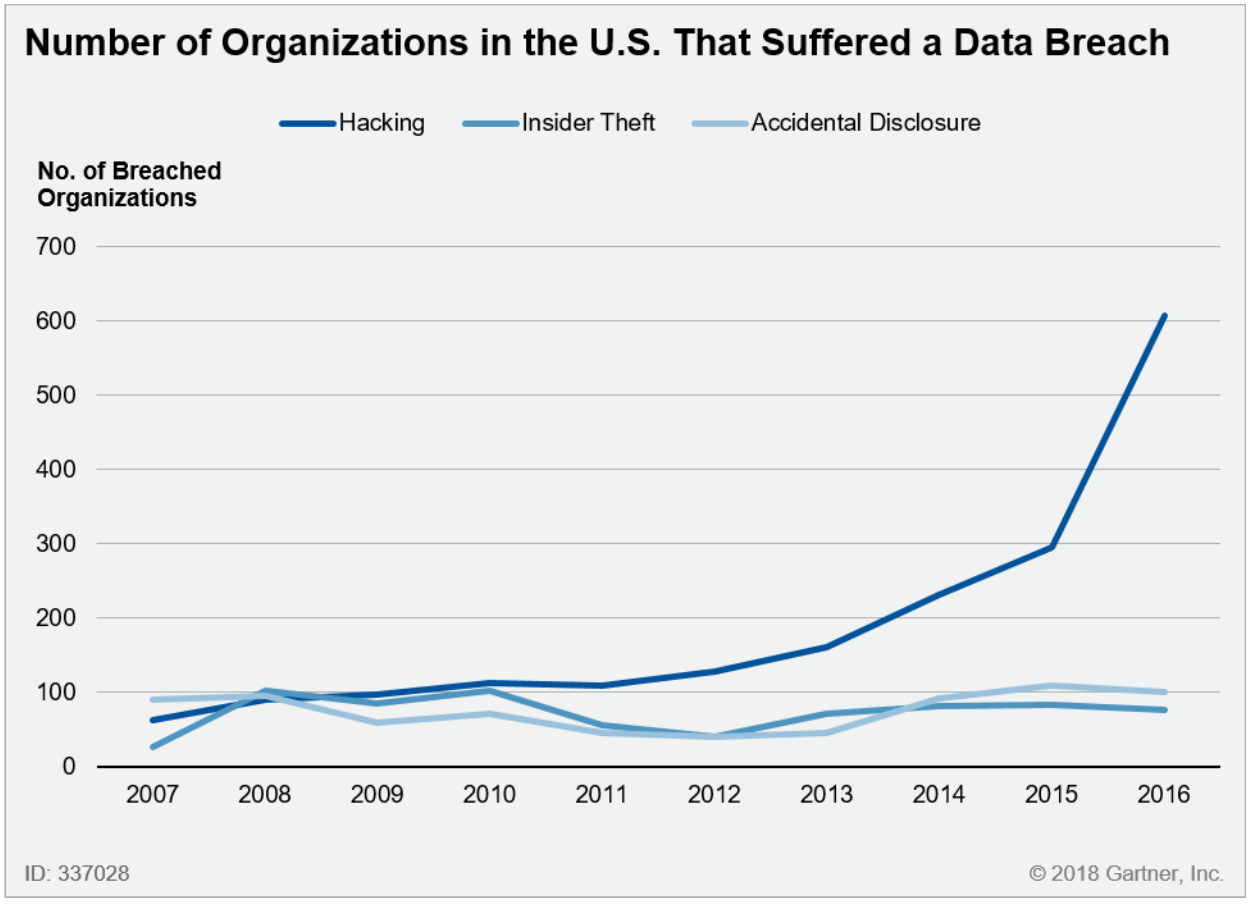
- Work closely with business stakeholders in pragmatic ways to build a security program that can link security strategy with business initiatives.

- Address the skills shortage at all levels with increased internal workforce development and other strategies.

Trend No. 2: Legal and Regulatory Mandates on Data Protection Practices Are Impacting Digital Business Plans and Demanding Increased Emphasis on Data Liabilities

Customer data is the lifeblood of ever-expanding digital business services. Incidents like the Cambridge Analytica use of Facebook data and the Equifax data breach illustrate the extreme business risk of data misuse. As the value of data increases, the number of organizations getting breached continues to rise (see Figure 2 and "Use Infonomics to Reset Data Security Budgets"). The resulting legal and regulatory environment, including Europe's General Data Protection Regulation (GDPR), is getting ever-more complex.

Figure 2. Number of Organizations in the U.S. That Suffered a Data Breach



Source: Gartner (April 2018)

These new legal and regulatory mandates are forcing massive changes on how businesses handle and secure customer data. The GDPR continues to expand customers' rights with respect to the handling, retention and distribution of their data. Customers have the right to view, rectify, delete

and restrict the usage of data, as well as rights to object to data storage and new rights to be notified of data loss. The GDPR also introduces new requirements for increased transparency around usage of data in automated processes. However, agile digital business will likely rapidly evolve automated processes with ever-more ML techniques, making continuous transparency about automated decisions challenging.

Organizations are facing growing risks to their data security as the number of data breaches continues to increase. Consequently, the tangible and intangible financial liabilities posed by regulators and cyberinsurers will also increase. Companies found in violation of the GDPR can be fined up to 4% of their global annual revenue. Equally important, the media coverage following breaches and fines could cause substantial damage to the brand's perception. Case in point, the controversy surrounding Facebook data immediately took 7% ($36 billion) off its market cap and substantially impacted consumer attitudes to the Facebook brand.

SRM leaders will be increasingly tasked with protecting customer data. New positions (such as chief data protection officers or chief privacy officers) are becoming more common. These leaders will be critical in guiding digital business decision making. In some cases, new legal and compliance requirements may lead to drastic changes to digital business strategies. Indeed, all digital business plans that include customer data must include increasing data protection costs and data liability considerations. SRM leaders should consider alternative options (such as using trusted third-party providers, anonymizing data or destroying sensitive data that is no longer useful). Leading organizations will use the urgency of the GDPR to redesign customer data life cycle management.

Recommendations:

To respond to rapidly changing requirements for personal data protection, security and risk management leaders should:

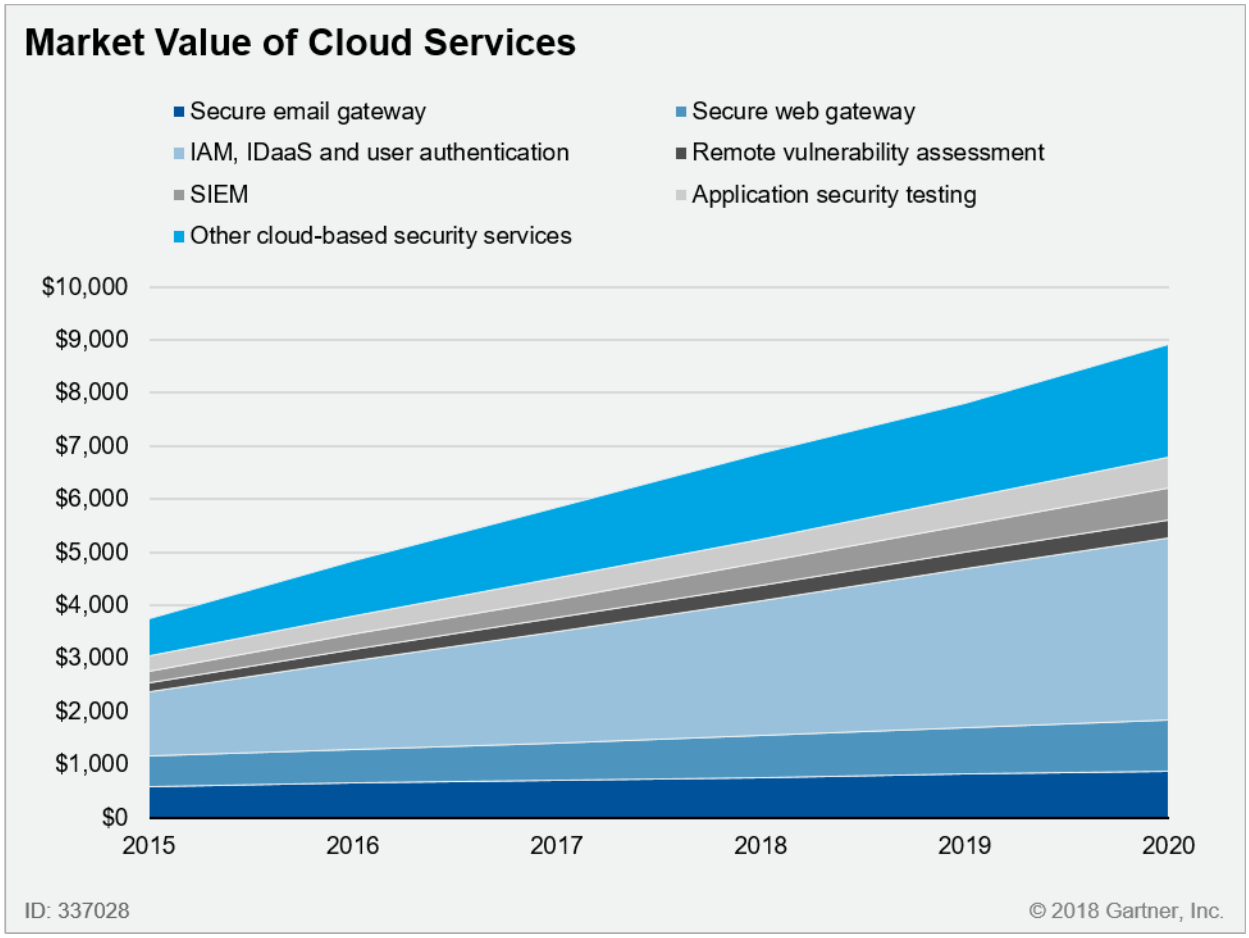
- Create compliance/privacy management programs and increase direct interaction in planning. Design these programs with business units pursuing digital business projects, particularly those that will involve customer or employment data.
- Approach compliance in customer interactions as a business enabler, focusing on the business value outcome. Use data transparency and protection as a market differentiator.
- Use the full liability costs of targeted data in digital business plans. Measure alternative options (such as using trusted third-party providers, anonymized data or established policies to delete sensitive data that is no longer useful).

Trend No. 3: Security Products Are Rapidly Exploiting Cloud Delivery to Provide More Agile Solutions

New detection technology (such as ML and user and entity behavior analytics), new activities (such as hunting and incident response), and adaptive authentication models require vast amounts of data that quickly overwhelm current on-premises solutions. Security product maintenance is overwhelming over-worked security staff. The shift to SaaS, IaaS and an increasingly mobile workforce are exposing the inefficiencies of network-bound security solutions. All of these factors

are forcing an accelerating shift from on-premises solutions to cloud-delivered security products (see Figure 3).

Figure 3. Market Value of Cloud Services



*Y axis is in millions, meaning $1,000 = 1 billion

Source: Gartner (April 2018)

Cloud-driven security services have significant advantages in addition to typical SaaS-value propositions. Effective cloud solutions will shift the administration burden from product maintenance to more productive risk reduction activities. The value of data increases with its telemetry, granularity and immediate global visibility. SaaS vendors can mine centralized data for new patterns and anomalies and to build and test new ML capabilities. Cloud-delivered security solutions can implement new detection methods and new services in a more agile way. Centralization of the management and data layer in a cloud service enables a provider to offer cost-effective staff augmentation services (such as hunting, posture assessments and incident response).

But not all cloud services are the same. Cloud product development is a different discipline from the traditional client server or local appliance. Cloud services should enable new techniques and services that exploit the unique advantages of the cloud scale, data consolidation and continuous

product evolution. SRM leaders should not assume that incumbent vendors will be able to successfully migrate to cloud delivery. Indeed, it is far more likely that incumbent providers will downplay the advantages of cloud until it is too late.

The primary barrier to adoption of cloud security solutions is the security, regulatory and legal implications of storing sensitive information in a third-party data center. For the vast majority of organizations, cloud vendors have a higher level of security and operational maturity. However, the concentration of data makes clouds more attractive targets for attackers. Prospective buyers must realistically weigh the risks to the business of breached cloud data. Buyers should also weigh data ownership and migration issues when considering the switching cost. Legal and regulatory hurdles are also a barrier to adoption. However, most cloud solutions providers can provide the same regulatory compliance assurances required of on-premises solutions.

Recommendations:

To avoid making outdated security purchasing decisions, security and risk management leaders should:

- Make a critical review of purchasing policy as it relates to cloud-delivered services to ensure that supposed barriers to adoption are material and factual. Force all purchasing decision makers to justify any new on-premises security solutions and ensure that at least one cloud-first solution was considered.
- Invest in solutions that deliver more agile solutions via a cloud and service delivery mindset over those that continue to use outdated product delivery methods.
- Seek out solution providers that:
  - Propose a cloud-first, cloud-intelligent architecture
  - Have a data management and ML competency
  - Offer services beyond break fix to staff augmentation
  - Can protect your data (at least better than you can)
  - Are API-driven

Trend No. 4: Machine Learning Is Providing Value in Simple Tasks and Elevating Suspicious Events for Human Analysis

As more security services move to the cloud and more cloud security services providers soak up more data, there are new opportunities to exploit ML to solve multiple security issues (such as adaptive authentication, insider threat, malware and advanced attackers). By 2025, ML for aspects of security will be a normal part of security practices and will start to offset some skills and staffing shortfalls.

Examples of ML providing value in security include vendors that have replaced the traditional signature database and have achieved acceptable levels of accuracy. Secure email gateway

solutions have been using ML since 1996. EDR solutions are using ML and analytics to spot anomalies. Banks and websites are using ML to improve protection from account takeover fraud. Gartner's continuous adaptive risk and trust assessment (CARTA) is a new strategy for dealing with the ambiguity of digital business trust assessments that will only succeed with ML approaches.

However, artificial intelligence (AI) and ML are overloaded marketing terms, making it difficult to distinguish between hyperbole and genuine value. Applying ML well enough so that it can actually detect something new and unexpected is very difficult. There are always outliers that result in false positives and false negatives. These will have to be interpreted by humans and used to tune the models. Effective ML must do more than previous generations of tools and must be durable enough to detect future threats.

In its current state, ML is better at addressing narrow and well-defined problem sets (such as classifying executable files). ML provides the best value when it is interpreted by humans, or when it enhances operator awareness by providing relevant information. ML helps short-staffed teams be more efficient, find threats they couldn't before, perform investigations more efficiently, and better anticipate future threats and risks.

But ML is not, and will never be, perfect. It is trained, tuned and refined continuously by humans, and often incorporates the biases and preconceptions of programmers. It can be gamed. Attackers will camouflage themselves in seemingly normal activity. There already are examples of trojanized good applications that can bypass machines. Attackers will evolve and move in directions not addressed by existing ML algorithms. The increasing availability of ML will allow attackers to exploit ML to improve their efficiency too.

We can't escape the fact that humans and machines complement each other and together they can outperform each alone. ML reaches out to humans for assistance to address intent uncertainty. ML aids humans by supporting administrator awareness and providing assistance to higher-tier SOC analysts.

Recommendations:

To take advantage of advancements in machine learning, security and risk management leaders should:

- Remember that unless a vendor outperforms competitors in a controlled test and can point at their ML implementation as the differentiator, it is difficult to unpack what is marketing from good ML.
- Ask the vendor how AI makes its product superior to current solutions in efficacy, and the administrative requirements of skill and time or other business metrics, as well as security metrics (such as dwell time and time to discovery).
- Demand a demonstration (not just a presentation) of how the vendor's product uses AI, especially using datasets indicative of the enterprise use case. Ensure that the demo is focused on how the solution improves business outcomes rather than simply showcasing functions or features.

Trend No. 5: Security Buying Decisions Are Increasingly Based on Geopolitical Factors Along With Traditional Buying Considerations

International borders have always been a friction point for security buyers due to regulations. However, increasing cyber warfare, cyber political interference and government demands for backdoor access to software and services have resulted in new geopolitical risks in software and infrastructure buying decisions.

The recent government[1] bans against Russian-based security products are the most obvious example of this trend, but there are numerous others. AT&T[2] dropped a smartphone manufactured by the Chinese firm Huawei. The U.S. moved to ban Huawei and ZTE from usage in government agencies.[3] The U.S. blocked the merger of chip makers Qualcomm and Broadcom due to security concerns.[4]

A global distrust exists toward the motivations and influence of competitive world powers that have started a cold war in cyberspace. Threat researchers have attributed the NotPetya[5] attack on the U.S. electrical grid and global election process to Russian state actors. Western governments suspect that China's National Vulnerability Database (CNNVD) includes secret, useful vulnerabilities that could be used for offensive purposes.[6] The U.S. National Security Agency lost control of its offensive weapons that were later used to devastating effect with the WannaCry ransomware attack.[7] In international relations, actors now wield technology as they have long wielded carrier groups and infantry divisions. NATO recently announced[8] that it will use cyber weaponry in NATO operations in the same way it uses conventional forces.

States are also ramping up their efforts to build police and national security backdoors into security software.[9, 10] Nation-states are using local jurisdiction to force solution providers to provide access to data stored in third-party data centers, even those that are outside its legal jurisdiction,[11] for law enforcement or national security interests.[12]

There have been several supply chain attacks[13] that illustrate the dangers of trusting suppliers to keep the environment clean. The NotPetya attack on Ukraine caused extensive collateral damage[14] outside the intended geopolitical boundaries. Intended or not, the disruptions that occur as nation-states launch cyber incursions throughout the world can be consequential to commercial actors, even if they are not the target.

Buyers need to be sensitive to the geopolitical security demands of its upstream and downstream business relationships. Companies that wish to do business with the federal government are not subject to the direction of federal agencies with respect to software restrictions. However, they might voluntarily comply to maintain standing with such a critical business partner.

The sheer scale of the hardware supply chain, not to mention the millions of lines of firmware in standard computing hardware, from IoT to mainframe, make it almost impossible to completely eliminate a geopolitical source in hardware. As software becomes more containerized and hosted on complex cloud software hosted in multiple geographies, the full-scale, top-to-bottom

geopolitical sourcing of software will also be impossible. Even today, security-conscientious organizations are starting to question the geopolitical location of insourced or outsourced consultants that contribute code to major suppliers.

All security and product buying decisions are based in trust in the integrity of the supplier. Solution providers will be considered responsible for the safety of their supply chain, although there is little evidence they will be capable of detecting supply chain attacks. Consider the recent Spectre and Meltdown vulnerabilities that affected millions of hardware devices across thousands of solution providers from all geographies.

Recommendations:

To avoid geopolitical risk, security and risk management leaders should:

- Incorporate geopolitical risk in all business critical of software, hardware and services purchasing decisions.
- Be aware of the geopolitical sensitivities of major business partners and consider the value of voluntarily following their guidance with respect to geopolitical risk.
- Consider local alternatives (such as T-Systems in Germany operating the Azure/O365/Dynamics data center).
- Start to include supply chain source questions in RFIs/RFPs and contract language.
- Focus security operations on detecting attacks based on behavior rather than inputs. Detecting lower-layer attacks will depend on monitoring for normal versus abnormal behavior of the system.

Trend No. 6: Dangerous Concentrations of Digital Power Are Driving Decentralization Efforts at Several Levels in the Ecosystem

The internet is currently driving a wave toward centralization. Internet digital trust is centralized in a few big providers in the form of certificates, domains and email providers. Cloud computing is concentrating the world's compute power in the hands of a cabal of powerful companies. The FCC recently replaced net neutrality rules, effectively concentrating access to internet content in the discretion of the major U.S. internet service providers.[15] The proposed merger of Thales and Gemalto[16] increases the concentration of hardware security modules, which are critical in high-performance cryptography, in the hands of a single French defense contractor. Centralization undoubtedly leads to economic efficiencies. However, as centralization gives way to monopolies and monocultures, the risk of disruptions and undesirable outcomes increases. Consequently, there is an effort to create decentralized alternatives. Blockchain is the primary technical enabler of decentralization, but there are others (such as Edge computing and peer-to-peer).

Concerns over centralized power and data privacy have fueled initiatives like Rebooting the Web of Trust.[17] This working group aims to develop security and privacy standards (such as Decentralized PKI,[18] and Identity Hubs),[19] which aim to exploit emerging technology (such as blockchain) to

decentralize trust and access decisions. Specifically, blockchain-based self-sovereign digital identity aims to introduce alternative methods to establish trust and resiliency with little reliance on centralized arbiters. The primary goal of these initiatives to provide end users more control over their identities and related attributes.

Edge, or Fog, computing moves computing resources away from centralized servers. Edge computing describes a computing topology in which information processing and content collection and delivery are placed closer to the sources and sinks of information. Information computing tasks are broken up into discrete IoT components (such as sensors, actuators and gateways) that act in a mesh to perform tasks.

Peer-to-peer (P2P) architectures are also on the rise after years of inattention. OpenBazaar created a P2P platform for e-commerce where there is no central intermediary. Mailpile is an email client that allows users to implement a decentralized self-hosted solution.

The ultimate goal of these decentralization approaches is to increase availability, security and privacy for users. Decentralized technologies are still an emerging area that will introduce new architectures that will need to be secured, and alternative methods to secure applications and data to enable more resilient services.

Recommendations:

Security and risk management leaders envisioning constraints on digital business plans as a result of a concentration of resources should:

- Evaluate the security implications of centralization on availability, confidentiality and resiliency on digital business plans.
- Explore an alternative decentralized architecture in digital business planning initiatives where centralization increases the risks to the business goals.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Develop Key Risk Indicators and Security Metrics That Influence Business Decision Making"

"Cybersecurity and Digital Risk Management: CIOs Must Engage and Prepare"

"Modern Privacy Regulations Could Sever or Strengthen Your Ties With Customers"

"GDPR Clarity: 19 Frequently Asked Questions Answered"

"Use Infonomics to Reset Data Security Budgets"

"Market Trends: Global Demand for Cloud-Based Security Is Growing Through 2020"

"How to Evaluate Cloud Service Provider Security"

"Market Insight: The Road to AI — A Journey to Smarter Security and Risk Decision Making"

"Questions to Ask Vendors That Say They Have 'Artificial Intelligence'"

"Maverick* Research: Living in a World Without Trust: When IT's Supply Chain Integrity and Online Infrastructure Get Pwned"

"Blockchain-Based Transformation: A Gartner Trend Insight Report"

Evidence

[1] On September 13, U.S. Government agencies were ordered to remove and replace all Kaspersky Labs product within 90 days. "DHS Statement on the Issuance of Binding Operational Directive 17-01," U.S. Department of Homeland Security.

[2] "Exclusive: U.S. Lawmakers Urge AT&T to Cut Commercial Ties With Huawei — Sources," Reuters.

[3] "Senators Push Bill Banning Chinese Tech Firms Huawei and ZTE From Being Used in Government," CyberScoop.

[4] The U.S. President blocked Singapore-based Broadcom Inc. from pursuing its hostile takeover of U.S. firm Qualcomm Inc., scuttling a $117 billion deal that had been scrutinized by the Committee on Foreign Investment, deeming it a threat to U.S. national security. "Trump Blocks Broadcom Takeover of Qualcomm on Security Risks," Bloomberg.

[5] "Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack," The U.K. National Cyber Security Centre. "NATO Cyber Center, DHS Probe Petya Attack," FCW.

[6] Recent industry reporting identified China's National Vulnerability Database (CNNVD) as a shell for the Ministry of State Security (MSS)-controlled China Information Technical Security Evaluation Center (CNITSEC). Multiple sets of data have suggested that the MSS filters reported vulnerabilities and likely reserves high-threat vulnerabilities for use in offensive operations. "China Evaluates Vulnerabilities for Attacks Before Disclosure," The Parallax.

[7] "What You Need to Know About the WannaCry Ransomware," Symantec.

[8] "NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons," Foreign Policy.

[9] "U.S. Says It Doesn't Need FISA Secret Court's Approval to Ask for Encryption Backdoors," ZDNet.

[10] "German government wants 'backdoor' access to every digital device: report," The Local.

[11] Clarifying Lawful Overseas Use of Data (CLOUD) Act would allow American law enforcement to obtain citizens' private data from servers anywhere in the world, provided they get a U.S. judge to

approve a subpoena. "CLOUD Act hits Senate to lube up U.S. access to data stored abroad," The Register. "H.R. 4943 — Clarifying Lawful Overseas Use of Data Act (CLOUD Act)," National Security Archive.

[12] "Twitter, Google Ramp Up Data Privacy Disclosure," Infosecurity Magazine. "Facebook Report Shows U.S. Government's Secret Requests for Data Shoot Up 26%," MarketWatch. "Russia's Supreme Court Orders Telegram Messenger to Hand Over Encryption Keys to Security Services," RT.

[13] "Lenovo Discovers and Removes Backdoor in Networking Switches," BleepingComputer.

[14] "Saint-Gobain Evaluates the Damage Related to the NotPetya Attack to 250M €," Le Monde Informatique. "NotPetya Ransomware Attack Cost Us $300M — Shipping Giant Maersk," The Register.

[15] "Restoring Internet Freedom," Federal Register.

[16] "Thales and Gemalto Create a World Leader in Digital Security," Thales.

[17] "Rebooting Web-of-Trust," Web of Trust.

[18] "Decentralized Public Key Infrastructure," GitHub.

[19] "Identity Hubs Capabilities Perspective," GitHub.

Note 1 Gartner Says Security Is a Board-Level Issue

See the following research:

- "Seven Keys to Successful and Cost-Effective Risk Oversight"
- "Toolkit: Board-Ready Slides for Security and IT Risk"

More on This Topic

This is part of an in-depth collection of research. See the collection:

- Research Roundup for Public Safety and Criminal Justice

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp