Security and Risk Management Scenario Planning, 2020

Published: 30 May 2013

Analyst(s): Paul E. Proctor, Richard Hunter, F. Christian Byrnes, Andrew Walls, Carsten Casper, Eric Maiwald, Trent Henry

Macro changes in targets and threats outside the enterprise are shaping the risk and security landscape over the next decade. Visibility into these anticipated changes will help strategic planning leaders dissect future security and risk practices and uncover new opportunities.

Key Findings

- As the targets for cyberattacks move between the enterprise and the individual, the threat landscape becomes more complex.
- As authority shifts between monolithic, central governments and self-organizing tribal communities, security strategies will have to adjust.
- Four scenario groupings mapped between targets to the enterprise and the individual and monolithic versus tribal authority represent the different dimensions of our future: regulated risk, coalition rule, neighborhood watch and controlling parent.

Recommendations

- Use Gartner’s preidentified leading indicators to understand which scenarios and forces will impact your business and customers.
- Prepare to address circumstances in multiple scenarios, because few organizations will have the luxury and clarity of experiencing only one.
- Plan and manage future control environments with a structured approach in any threat context (see "Four Strategies for Optimizing Your Security Controls in Future Scenarios").

Table of Contents

| Strategic Planning Assumptions | 2 |
| Analysis | 2 |
Strategic Planning Assumptions

By 2020, risk assessment will drive more risk and security spending than government regulation, despite increasing government regulation.

By 2020, 25% of global enterprises will engage the services of a "cyberwar mercenary" organization.

By 2020, at least one consumer product manufacturer will be held liable by a national government for security vulnerabilities in its product.

By 2020, Facebook will lose 30% of members who have been with the site for more than three years due to privacy concerns.

By 2020, 30% of CEOs for Global 2000 companies will have been directly compromised by an independent group of cyberactivists or cybercriminals.

Analysis

Background

In February 2013, a group of 12 Gartner global thought leaders met in San Diego to share, scrutinize and map the long-term future of security and risk management practices. They conducted a
scenario-planning exercise that led to the creation of forward-looking tools and strategies — viewed through a completely new lens — for navigating through 2020.\(^1\)

The Gartner exercise defined major forces of a plausible risk landscape, diagnosed change agents and pinpointed probable scenarios. From these scenarios, Gartner identified the leading indicators within each scenario — critical forthcoming events, behaviors, policies and actions — that are likely to affect business and customers. Leading indicators may point to business risk or suggest new revenue and service avenues.

The results of this work can inform risk and security leaders with their own strategic planning. By recognizing key, leading indicators, organizations can see emerging patterns, better prepare for adaptation and tailor progressive plans of action (see Note 1).

**Scenario Introduction**

The scenario is defined by two major forces. Each force is described as a continuum from one extreme to the other. When presented orthogonally, they create a graph that defines four different scenarios (see Figure 1).

**Figure 1. The Gartner Security and Risk Management Scenario**

Source: Gartner (May 2013)
Reality always lies between the extremes. Most organizations will experience circumstances present in multiple scenarios when viewed through the widest angle. A keen understanding of the forces — combined with a recognition of the scenarios most likely affecting your business — will help establish the foundation for guidance.

- **Force 1**: The target spans from enterprises to the individual (see Figure 2).
  - Enterprises have traditionally been the target, but sophisticated threats to the enterprise are increasingly occurring via soft targets in individuals — individuals who are employees, customers or citizens.
  - Examples of individuals as the target include smartphone vulnerability exploitation and spear phishing for executive credentials.

**Figure 2. Scenario 2020, Force 1**

Security compromise of enterprise accounts may become more heavily weighted to indirect attacks through captured end nodes, or may focus even more clearly on servers.

![Diagram showing target spanning from enterprise to individual](image)

Source: Gartner (May 2013)

- **Force 2**: The authority measures across the monolithic (government) to the tribal (collectives) (see Figure 3).
  - Historically, governments use regulation to influence corporate behavior, but increasingly, Gartner observes collectives of like-minded entities banding together.
Examples of collectives include Industry consortiums such as the Payment Card Industry (PCI) and Bits (the technology policy division of the Financial Services Roundtable). A less obvious example of a collective is parental Web-control products that can be tied to a group of concerned parents as the driver.

The authority force line also applies to attackers for both the monolithic side (such as nation-state-sponsored hacking) and the tribal side (for example, the Anonymous hacking group).

Figure 3. Scenario 2020, Force 2

The level of market intervention can vary dramatically, shifting costs and influencing business flexibility.

Source: Gartner (May 2013)

Creating Four Scenarios

The relationship of the two forces to one another is shown by two interacting axes creating four, distinct grid areas. Each grid contains a scenario that should become part of your strategic plan for security and risk management. Each scenario is described by the results of these two interacting forces.
The scenarios are regulated risk, coalition rule, neighborhood watch and controlling parent (see Figure 4).

**Figure 4. The Four Scenarios for 2020 on a Grid**

How we select from and apply our four control strategies will depend on how the world changes for our organization.

Source: Gartner (May 2013)

In these scenarios, you will be able to:

- Identify some of the threats and opportunities resulting from movement into a scenario.
- Interpret the scenario based on present-day evidence.
- Understand how to recognize when you are experiencing the scenarios by their characteristics.
- Use the leading indicators to trigger planned changes to your control portfolio and security posture.

Gartner research will continue to monitor shifts and will continue to provide guidance on responses. Additional research will provide more in-depth responses to each scenario based on current position. Below, we describe each scenario, how to recognize it and how to appropriately address each one (see Figure 5).
Scenario 1: Regulated Risk

This scenario is most like what organizations feel they are experiencing in 2013, with targeting remaining squarely on the enterprise, and increasing regulation guiding enterprise actions and forcing security department focus. Governments will attempt to use regulation to provide safety to the enterprise and to itself. All infrastructure becomes critical infrastructure; enterprises are held responsible for the actions of their employees. Attacks can become acts of war. The extreme of this scenario is outright cyberwarfare between governments.

Threat: More regulation increases cost, but does not necessarily decrease risk.

With increased regulation comes increased cost in capital expenditures and business impact through regulatory distraction. Compliance will continue to be a primary driver, and this will reduce resources on risk assessments to prioritize and address real enterprise risk.

Opportunity: Government intervention will materially impact cybercriminals.
Increased government involvement in attack traffic may more effectively block and take down bad actors, such as botnets. More cybercriminals will be caught, raising the opportunity cost for those seeking to take advantage of organizations.

**Present-Day Evidence**

Clearly, increased cyberlegislation, such as the cybersecurity presidential order in the U.S., the focus on critical infrastructure protection directives, and increased news regarding cyberwarfare between nations are signs that elements of this scenario are present in 2013.¹

**Leading Indicators**

The following indicators will presage a move deeper into the regulated risk scenario:

- New regulations
- Increase in public acknowledgment of attacks
- Increase in government disclosure of breach info
- Public shaming and fines for breaches
- Publication of a "Monroe Doctrine" for cybersecurity rules of engagement
- NATO creates a cybersecurity division
- Software liability established
- International convention on cyberwar, and one major nation refuses to sign because it limits its responses

**Recommendations**

- Identify and protect strategic assets of your organization.
- Create a balance between regulatory compliance and effective risk management.
- Avoid increased regulatory distraction by building a proactive set of risk controls based on good risk assessment, and then map those controls into regulatory requirements.

**Scenario 2: Coalition Rule**

This scenario is characterized by continued attacker focus on the enterprise, with a de-emphasis on following central authority as rules are deemed ineffective. The attacker perspective on the authority force comes into focus as autonomous collectives of freelance/mercenary hackers (cartels) proliferate, and hacktivism escalates. Major corporations (warlords) will establish protected cyberfiefdoms and the cost to participate explodes. Warlords and cartels will rule.

**Threat:** An increase in attacks could cause severe damage to business.
There will be less government scrutiny and distraction, but cybersecurity costs are likely to escalate due to factors such as aggressive corporate and national espionage. The underground cybercriminal economy will grow, resulting in more losses, and the defensive cartels will exact their own prices to participate in their protection. The supply chain for offensive activities available to both the attackers and the defenders will grow. Governments will not monopolize the attack activity because enterprises will create their own capabilities to respond to attacks by targeting their adversaries.

**Opportunity:** Establish, then dominate an industry standards group.

In this scenario, the opportunity for enterprises is to align with or drive one of the cyberfiefdoms in the form of an industry collective group or alliance. These alliances will bloom to share attack information, protective controls and even counterintelligence/counterstrike activities.

**Present-Day Evidence**

In 2013, industry collectives and attacker collectives are everywhere. Examples include the Cyber Security Alliance, Cloud Security Alliance and even criminal gang use of the Internet. Published findings of cybercriminal activities from research wings of anti-malware vendors indicate a continuing increase in organized attack activity by self-organizing groups and governments. Emerging research on offensive misinformation techniques and courses being taught to white-hat security professionals in offensive control methods point to increasing interest in a willingness to apply offensive techniques.²

**Leading Indicators**

- Evidence of corporate counterattack
- A major financial services firm or bank forms its own cyberwar department
- Initial public offering for cyberwar mercenary company
- Increase in crypto-extortion schemes
- Cyberinsurance fails and is withdrawn
- Public corporation records $100 million charge for cyberblackmail

**Recommendations**

- As government regulation fails to make any material difference, it is even more important to define real threats to the enterprise and act aggressively to address them.
- Acquire and retain the best technical security talent possible, but manage them proactively.
- Align with industry consortiums that provide concrete benefits like attack data sharing, and shun those that offer weak benefits, such as a framework to follow.
Scenario 3: Controlling Parent

This scenario is characterized by individuals (customers, employees and citizens) as the target, and increasing regulation. Increased attacks against individuals will force governments to act. Criminal use of data mining is used to identify potential victims, and strong privacy regulations will emerge. The controlling parent is the government, which will step in to protect the individual, and create distraction and limit opportunities for businesses. As the individual is increasingly targeted, enterprises will need to respond with new controls to address customer concerns and satisfaction.

**Threat:** Privacy regulations will inhibit business operations.

As theft-oriented botnets proliferate, governments will try to establish norms of personal responsibility. An explosion of privacy regulation will not only impact controls and security activity, but will also have a material impact on innovation as companies are restricted in their use of data to build their businesses, and product opportunities are stifled due to onerous control features on products.

Individuals call for government assistance in "making the Internet safe for children," and this increases government intrusion into cyberspace. Government regulation increases surveillance to find wrongdoers (or bad actors) and limit the pain felt by citizens.

**Opportunity:** A surveillance society benefits those who do privacy and big data well.

As the government surveillance society grows, resulting in pervasive Internet activity tracking, a darknet where individuals can conduct business will expand from the paranoid to the everyday citizen. Companies can create competitive advantage by offering private and protected access to online services. Mobile devices will become closed and curated, such that business will have to create more proactive, protected and private connections to individuals. All this will happen with government sanction and approval. Companies that can anonymize and take advantage of big data appropriately will thrive, while those who run afoul of harsh privacy regulation will be fined and suffer increased scrutiny.

**Present-Day Evidence**

Examples of the controlling parent are present and growing in 2013: in the U.S., the Do Not Call List, the Foreign Intelligence Surveillance Act (FISA) amendments, moves to implement licenses for individual Internet use, authority trying to influence individual behavior in cyberbullying, reporting on identity theft, and court rulings that deny offensive computer investigative techniques. In Europe, the EU data privacy directive is a good example.3

**Leading Indicators**

- ISPs (outside of Europe) ordered to retain all transactions
- Consumer Product Safety Commission (CPSC)/Federal Trade Commission (FTC) takes action against product vulnerabilities
- U.S. class action lawsuits over vulnerabilities
School training and (in some areas) licenses to get on the Internet
Creation of computer user databases by governments

Recommendations

- Create a connection between privacy protection and product management to protect and take advantage of the privacy environment for competitive advantage.
- Expand controls to protect customers, citizens and employees from the proliferation of attacks targeted at the individual.
- Invest in people-centric security controls to change individual behavior and improve risk posture.

Scenario 4: Neighborhood Watch

The neighborhood watch scenario is essentially anarchy as individuals are increasingly targeted, and decreasing regulation signals that government intervention is not going to materially impact the situation. E-militias will form to protect against extreme anarcho-hacktivism. Corporate and communal interest groups will stand up “walled gardens” (for example, protected enclaves where members can operate safely within the confines of the protective boundaries) and self-organizing protection societies (honest and dishonest) will flourish.

**Threat:** E-commerce will drop, and the utility of corporate reputation and consumer trust will diminish.

Individuals will band together with others like themselves (the actual criteria for groupings will vary), and they will trade or work among themselves. Trade between groups will only occur for mutually beneficial activities or after trust has been created. Individuals will make extensive use of darknet services and depend greatly on anonymity. E-commerce will decline because of distrust, and major civil cyberstrife will be commonplace.

**Opportunity:** Form your own protection society for your customers.

In a world driven by protection societies, the opportunity is to create your own. Providing anonymity and a safe environment for your customers will top customer service requirements. Learning to work effectively within an expanding network of walled gardens will separate the winners from the losers in business.

**Present-Day Evidence**

- Walled gardens of the Internet
- Currency markets on the Internet like bitcoin that allow criminals to exchange funds anonymously
- Rise of individuals targeted in identity theft, cybercrime and fraud
Fake reports of news on social media from hacked accounts of legitimate media sources

**Leading Indicators**

- Formation of cybermilitias
- Groups like Anonymous focus on CEOs rather than business operations
- Corporations start refusing to hold personal information
- Harassment, reputation attacks and cyberbullying become common
- Facebook loses 10% of its members
- Slowdown in e-commerce growth rate

**Recommendations**

- Create a customer environment that ensures and promotes electronic safety.
- Build relationships and controls that extend online safety to your partners and suppliers.
- Adjust business practices to address the reality of a slowdown in e-commerce.

**Recommended Reading**

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

"Four Strategies for Optimizing Your Security Controls in Future Scenarios"

"Expand Business Continuity Management Efforts to Deal With the 'Coalition Rule' Scenario"

"Let Go of Personal Data Without Losing Control"

"Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence"

**Evidence**


2 Excerpt from SAN's *SEC440: 20 Critical Security Controls: Planning, Implementing and Auditing,*
"One of the best features of the course is that it uses offense to inform defense. In other words, you will learn about the actual attacks that you’ll be stopping or mitigating. That makes the defenses very real, and it makes you a better security person."


A. Greenberg, "Meet the Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)," Forbes.com, 21 March 2013.


J. Tuckman, "Internet Becomes a New Battleground in Mexico's Drug Wars," Guardian.co.uk, 31 October 2011.


J. Pachin, "Educating Students about the Consequences of Cyberbullying and Sexting," Cyberbulling Research Center, 8 April 2013.


Note 1 Scenario Planning Explained

- Business and technology leaders may experience uncertainty derived from the Nexus of Forces in mobile, social, cloud and information technologies.

- Scenarios are compelling descriptions of possible futures outside the control of an organization. They are not necessarily the most probable events, but plausible and coherent ones discovered through logical extension of present-day occurrences and behavior.

- Scenarios are not predictions nor contingency plans, and they are not the same as strategic options. Strategy — and the successful execution of it — are within an organization’s control. Scenario planning may help leaders visualize what would happen if the company innovated in a particular direction and plan how to best react to these possible outcomes.

- Indicators are litmus tests for the direction of scenarios. Indicators are not milestones in traditional scenario planning. Milestones suggest progression. In risk and security scenarios, progression is complicated by the forces themselves. It is possible — based on present-day evidence — that no one scenario will dominate over others, but that an awareness of all indicators will lead to better adaptive practices.

More on This Topic

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

- Long-Range Planning Guidance for Information Security and Risk Management: Gartner’s Security 2020 Scenario