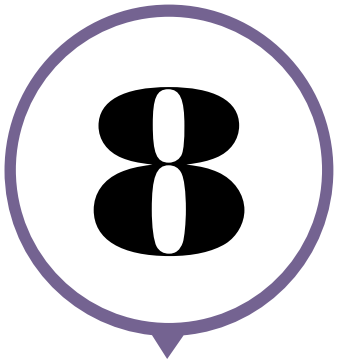
SPACE TAKEN FROM PREVIOUS CONVERSATION



SECURITY

In an increasingly interdependent and dynamic world, the array of possible threats and risks is rapidly evolving. Clashes between different political and social ideologies remain a concern, while securing access to vital resources is re-emerging as a potential source of conflict.

The nature of conflict itself has changed, too, with new technologies, such as unmanned drones, and increasing use of new urban guerrilla tactics. A new dimension is the need to look beyond overt physical threats to smaller-scale and more intangible risks, such as politically-motivated vandalism and cybercrime. Such threats might not risk the stability of a nation, but they might potentially cause distress and inconvenience to huge numbers of people. With these shifts come changes in approaches and methods for keeping secure.

Where's the heat?

/ Peace and reconciliation
/ Terrorism
/ Changing nature of warfare
/ Defense industry
/ Arms proliferation
/ Crime
/ Cybersecurity

/ **Peace and reconciliation**
Economic development is seen as key to creating lasting peace in troubled regions. It used to be said that no two countries with a McDonald's ever went to war – until the Russia-Georgia conflict of 2008.

/ **Terrorism**
The US spends more on counter-terrorism than all other anti-crime activities. Governments are struggling to find the right mix of hard power combined with diplomacy and strategic aid.

/ **Changing nature of warfare**
At the start of the last century, land warfare using infantry dominated. Now, guerrilla tactics and terrorism demand increasingly sophisticated, precise and technologically advanced responses.

/ **Defense industry**
Defense spending can be a major part of a country's economy – 4.5 per cent of GDP in the US in 2010. Some argue the industry creates employment and fosters innovation, though others raise concerns about the ethics and political say of the "military-industrial complex."

/ **Arms proliferation**
Controlling the spread of arms requires an ongoing series of multilateral talks and agreements. The illegal trade in small arms is estimated to be worth between $2bn and $10bn a year.

/ **Crime**
Global organized crime is worth $1 trillion a year. Aside from the human cost, it damages economies: drug-related violence costs Latin American countries the equivalent of nearly 15 per cent of their GDP. At the other end of the spectrum, low-level antisocial behavior undermines local communities.

/ **Cybersecurity**
Two in three internet users have been affected by cybercrime. Cybersecurity has become a matter of national security as hackers from hostile governments could wreak havoc on critical infrastructure. In 2010, the Pentagon set up a new US Cyber Command.

What's the context?

Hacking is a familiar word, but it comes from a subculture most of us know little about. Hackers have their own ethics and language. They have a natural suspicion of authority and secrecy, and place a high value on information sharing and openness. Hackers love the challenge of stretching a system to its limits and pushing its capabilities.

Of course, hacking has become indivisible from cybersecurity. For most people, hacking is the digital equivalent of breaking and entering: finding weaknesses in a security system and exploiting them. There are broadly three different motivations for doing this.

"Hactivists" are motivated by political or ideological reasons, and include groups such as Anonymous in the US or the Red Hacker Alliance, a network of Chinese nationalist hackers.

"White hats" are hackers who seek out flaws in security systems so they can be fixed. The group LulzSec, for example, hacked into the British National Health Service – but alerted administrators to the vulnerabilities.

"Black hats" are more problematic. They are motivated by personal gain, or just pure maliciousness. They're often after financial data such as personal banking information, and they're a big threat to the financial services industry.

Hacking has become so advanced that cyberspace is now thought of as the "fifth domain" of warfare – alongside land, sea, air and space.

> The same global advances in communication, transportation and commerce that lead to economic growth, social exchange and political integration can also be conduits for transnational security threats
> — The Brookings Institute

> Violence has been in decline for thousands of years, and today we may be living in the most peaceable era in the existence of our species
> — Stephen Pinker, psychologist and author

> We are in an information war and we are losing that war
> — Hillary Clinton, testifying to Congress

ELLEN RICHEY
Chief Enterprise Risk Officer, Visa

DOUGLAS MICHELMAN
Global Head of Corporate Relations, Visa

Activist groups, such as Anonymous, are drawing public attention to fast-changing cyber security threats. For companies such as Visa, the international payments group, security is at the very core of what they do. Here *Ellen Richey,* a lawyer with considerable experience in the financial services industry who is now Visa's Chief Enterprise Risk Officer, and *Douglas Michelman*, who as Visa's Global Head of Corporate Relations is chief protector of the firm's reputation, explain to Joe Carberry how companies can stay a step ahead of cybercriminals.

Is the world a more dangerous place than it used to be?

Ellen Richey: It can certainly feel like it. But I believe our world is not significantly more dangerous today than, say, 10 or 20 years ago. In many ways, we are actually more secure. But I think it is fair to say that our world is far more dynamic, and the risks we face evolve more quickly.

There seem to be more and more stories about cybercrime and other high profile threats. Does that reflect reality?

Douglas Michelman: When people see story after story about new risks they can seem more immediate, more dangerous or

50m

The military is recognizing the value of training technology: in 2008, the US army decided to invest $50m over five years in gaming systems designed to prepare soldiers for combat

1 trillion

It has been estimated that cybercrime costs businesses at least $1 trillion a year in lost intellectual property and damage repair costs

more localized than they actually are. This raises the attention level leading to dialogue and, in some cases, alarm. Given our fast-paced and interconnected media environment, organizations must be prepared, visibly and aggressively, to address any security issues they might face, real or perceived.

What does it take to protect other people's money every day across the globe?

ER: Visa processes about 71bn transactions a year in nearly 200 countries and more than 175 currencies. Keeping fraud rates at an all-time low at that scale is no small feat, and there is no single correct answer. At Visa, we describe our approach as "layered defense." We employ multiple, interconnected security measures that work together – things like technology, policies, physical security, point-of-sale procedures, consumer alerts, monitoring and rapid response to events.

How does the proliferation of technology affect security?

ER: Like every aspect of our lives, technology has a huge impact on security. The downside is that new technologies can create new risks. It can also make those with bad intentions better at what they do. Criminals today are smart, innovative and well financed.

The good news is that technology is also a huge asset for those with good intentions. Technology makes us better at what we do and remains one of our most effective assets to fight fraud. Our data centers are a great example. Inside these massive complexes we have some of the world's most sophisticated technology dedicated to rooting out fraud. We can spot unusual patterns in real time and stop fraud before it occurs. We stay ahead of criminals with these kinds of investments. As a result, we've driven fraud to an all-time low – a clear sign we are still winning the war.

How can an organization use security to build trust?

DM: For Visa, we have to drive the discussion of what future solutions look like. So we've created a series of activities that help demonstrate our long-term commitment. In 2005, we hosted the first Visa Security Summit, bringing together hundreds of experts from business, academia and government to create a dialogue around our collective issues. We've now held four summits in the US and several dozen others in places as diverse as São Paulo, Toronto, Cairo, Dubai and Jakarta. Similarly, we've hosted educational forums and developed online tools to help foster security. We have even featured security prominently in our marketing. Together, these efforts have set a high bar for payment security and, importantly, have built trust in Visa.

Trust is an important bridge to future innovations, such as mobile banking. For example, a recent study [*US Federal Reserve Report: Consumers and Mobile Financial Services,* March 2012], shows that 42 per cent of people cite security as the reason they had not adopted mobile banking.

Why do you think security has become such a hot topic for so many people and companies?

ER: Security interests people because it involves things going wrong, sometimes in very big ways. Security is a complex subject and defies a simple definition. It encompasses a wide variety of areas. Organizations must protect themselves from the impact of international conflicts, criminal activity, natural disasters, equipment failure, new forms of technological attack, and human error, among other threats. Security's meaning differs by person and by industry and changes over time. Each organization has its own unique combination of risks to combat.

How do you strike the right balance between managing risk and pursuing opportunity?

DM: With any new venture, an organization must weigh risks and rewards. When they do, companies should make decisions as if their most important stakeholders were there in the room with them. At Visa we are guided by a concept known as "responsible innovation." This reflects the fundamental choice our company makes every day. We are a company that uses technology in new and innovative ways, but we also have significant amounts of sensitive information in our care. So when we develop new ideas, we have to keep in mind the difference between what is possible and what is responsible.

People have high expectations for organizations like yours, that you'll safeguard their information. Are those expectations realistic?

DM: I hope people never stop expecting the best from us in this area. Our job is to live up to high expectations, and, in some cases, set the bar even higher. We engage with our stakeholders to ensure two things. First, we want them to understand all we do to secure our system and their information. We work with a wide variety of constituencies – from lawmakers and law enforcement to industry and consumer groups – to ensure we understand their expectations and how we can meet or exceed them. Second, we want them to understand where our role ends and theirs begins. Each of us has a role to play; security is a shared responsibility.

Can you ever be truly secure?

ER: Any risk management professional would tell you it's impossible to eliminate risk entirely. But it can be successfully managed. For example, we encrypt data to protect it from theft or misuse. We also put programs in place to protect our customers in case something bad happens. These kinds of steps go a long way toward our fundamental goals: first and foremost, to secure our system, and second, to maintain the trust that our stakeholders place in us to keep them secure.

Joe Carberry *is a Partner in Brunswick's San Francisco office. He advises on privacy and data security.*