

Impact of Terrorist Attack on Technology

Rob Enderle

Giga Position

Catastrophic events often result in behavioral changes that can be mapped over time. When technology is in place to enable these changes, they can happen very quickly; when it isn't, the change can fuel an accelerated level of development to meet a new set of needs made recently critical to the buying population. The attack on the World Trade Center and Pentagon was the beginning of what is likely to be a series of events that will fuel a rapid change in behavior that should favor companies like **IBM** and **Polycom**, which have invested heavily in the technologies many will need to both meet their needs for safety and productivity. Firms primarily focused on price, like **Dell**, will be at a disadvantage as they attempt to catch up.

Looking forward, as hostilities escalate, we would expect the result will be a fundamental change in the way companies provision employees, handle security over intellectual property and collaborate. Technology purchases should anticipate these changes and reflect an increased risk surrounding emerging technologies in favor of those that currently can be deployed. For the near term, personal security will likely be a driving factor in most decisions, and that should be enough for these events to be a strategic inflection point.

Proof/Notes

Intel's Andy Grove defined a strategic inflection point as a change so powerful that it fundamentally alters the way business is done. Most of these have been obvious after the fact but entirely missed or misinterpreted at the time of the actual events. When such an event occurs, the impact can be accelerated by the existence of technology that addresses the concerns raised by the event or by the rapid development of such technologies. The recent attacks on the World Trade Center and Pentagon, coupled with the US reaction to those events, have the potential to be viewed as a strategic inflection point.

To look at the impact of this inflection point, we need to move ahead into 2002 and create a view of the United States, and much of the Western world, that will be likely in that time frame. Giga expects the following environmental changes will drive much of the market during the time the "war" is active and that these changes will define purchasing priorities and both winners and losers as the event matures.

Travel

Travel will have become vastly more difficult — wait times to board planes will average several hours and the ability to arrive less than 30 minutes before a flight and actually get on it will be virtually nonexistent in most airports. Executives who have been able to traditionally overcome this problem through the use of private jets will suddenly find there are sharp restrictions using them as many will have to be updated to prevent their unauthorized use as weapons delivery platforms. (Currently, private planes reside in areas that are not as well protected as public air transport and have nearly the same potential, particularly in international configurations, for destructive use as their larger siblings.) Turning a four- to eight-hour trip into an eight- to 12-hour trip, much of which is spent in limbo with the occasional break for a physical search, will be very distasteful to people raised in the US and should result in a sharp decline in airline use and create the potential for dramatic restrictions on small regional airports and the use of private jet aircraft. (At the time of this writing, private aircraft are grounded.)

A number of companies have already adopted policies that will remain in place during the threat that will

make air travel for their US employees nearly impossible. Travel overseas, for many, will likely be curtailed for an even longer period as those with US passports become aware of both their personal risk and the inability of the US government to protect them while in Europe, or in some cases, in the air.

In addition, those who continue to travel and carry large items on planes, particularly items that could conceal weapons or explosives (like laptops) will experience longer wait times as this hardware is physically inspected and, depending on how the inspections are done, there may be an increase in related breakage. On the other hand, small devices like cell phones and personal digital assistants (PDAs) may gain wider acceptance because they, in the case of cell phones for instance, actually represent a benefit (given their use during the initial attack) or a reduced risk because of their size.

With the government currently sending out alerts that fire trucks may be stolen, converted into bombs and used much as the jets were used in the Sept. 11 attack, travel in and around cities will likely experience some restrictions as well. In these locations, the general atmosphere around any kind of travel will likely favor offices in rural areas close to employees' homes, in homes or other electronic alternatives to physical travel.

Security

Because of the massive loss of life and property, there will be a shift in how we secure our buildings and personal equipment. Previous to this event, security efforts focused on protecting intellectual property from theft. This reduced the emphasis on backups and drove technologies like encryption as the primary means for providing this protection. Even when backups were done, there was very little testing to make sure that they were done properly so that the information could, in fact, be recovered. In 2002, the focus will be more on protection against loss rather than theft. This enables technologies like backup and synchronization and focuses more on legal rights as the way to protect intellectual property from theft. In addition, it raises a level of risk around encryption that may be unacceptable to some. Executives that rely primarily on an encrypted PC represent a much greater risk if they die — even if the computer itself is recovered, it is almost impossible to gain access to the contents if they have been effectively encrypted, and no one but the executive knew the password.

Personal security will clearly be vastly more important, and two-way pagers, cell phones and other wireless technologies, some integrated into global positioning systems (GPS), which can allow people to effectively call for help and/or quickly determine the location and safety of loved ones or employees, will be much more easily funded. When personal security is threatened, even if that threat isn't realized, behavior, particularly purchasing behavior, often changes. People will either move to products that improve their feeling of security or they husband their resources. Existing products will either be effectively repositioned to meet this need or face a strong decline in relative demand and sales. Discords, messages that are dramatically opposed to perceptions, will likely backfire. For instance, the recent government push to get people onto airplanes before the airlines have been able to fully check security staff or correct the physical security problems may result in another disaster, and the consumer response to such a scenario, were it to occur, would undoubtedly be near terminal for the entire industry.

With concerns about personal security likely fueling domestic personal weapons sales and impending large-scale layoffs undoubtedly resulting in an increase in employee-related violence, the opportunity for serious problems at large sites, particularly those with Middle Eastern employees who may be targets of any attacks, is likely to increase dramatically as we enter the new year. Hate crimes are already up sharply as fear is translated into inappropriate violent action. Already some sites have instituted armed guards, metal detectors and other means to keep weapons away from corporate offices. Existing methods of identifying employees will likely be seen as inadequate, particularly given the use of false identification by the hijackers. This should fuel a strong effort to both integrate security offerings and tie them more securely to the actual employee. We continue to feel that the best approach is a combination smart-card/biometrics approach where the biometric component validates the connection between the card and the employee. This same method will likely find its way into system security schemes both to keep it simple and to better ensure that people who

are accessing systems are both authorized and accountable for that access.

Buildings, particularly window-wall buildings in large urban areas carrying a well-known US brand, that are directly off of public streets or directly attached to parking lots will increasingly be seen as higher risk than those in rural areas with a large perimeter that can be monitored and protected. This should shift funding from large, highly visible, urban edifices to more visible virtual sites and undoubtedly fuel the need to relocate to rural areas for a large number of businesses. Along with this should be a greater interest to provide for employees to work from home, since those employees will likely be the most secure and least impacted by any activity targeted at a corporate site or related location.

Video monitoring was already being deployed in some cities and the objections to that technology have dropped off sharply in the face of this new threat. In addition, the US Department of Justice (DOJ) has requested that privacy rights be dramatically reduced to allow a much more broad monitoring capability for all types of communication. While this is currently meeting strong opposition, if the expected additional attacks occur, this opposition will likely decline sharply allowing these changes. This expanded capability, once in place, could be used in investigations into corporate practices. Overall, privacy rights, personal or corporate, will likely have declined sharply by mid-2002. Certainly technology that can do data mining on this kind of media or otherwise automate what otherwise is likely to be a very tedious process will receive substantially more development funding and sales.

Impact

While this scenario depends on the continued conflict and the resulting US domestic risks associated with this conflict, were it to end, the long-term impact of the World Trade Center attack would be reduced but not eliminated. For this next section, our assumption is the conflict will not be quickly settled, and the current trends will continue into 2002.

Product Casualties

Sales for products that are not focused on safety and security will fall off sharply. PCs, Windows XP, consumer electronic products and a broad cross section of products focused on general corporate and personal needs will decline in favor of products and services that increase the security of the individual and the corporation. Some products, like Windows XP, might be able to be repositioned to address some of the electronic security concerns; however, the launch campaign is largely complete, and there is little time to effectively change the core messaging. This means that while we still believe a market recovery is likely in 2003, the recession in this market will be much deeper than otherwise would be the case.

Potential Successes

Fighting this trend will be products that increase the ability for people to communicate, avoid travel and increase personal, corporate and intellectual property security. Companies like IBM that have quietly made security a central focus for years may be immediate beneficiaries. Video conferencing, cell phones, wireless handheld computers, employee authentication systems (particularly those with biometrics and that integrate site security with electronic access security), video surveillance systems, disaster protection vendors, backup systems, multimedia streaming, targeted data mining systems and related services are obvious beneficiaries. Game machines like the Microsoft XBox and **Nintendo** Cube may meet expectations as people look for ways to do virtually what they cannot do physically to deal with the threat. Increases in the use of telepresence should be dramatic as the inability to safely travel pushes substantial additional funding into this emerging field. In addition, services related to moving data centers, securing corporate sites, increasing redundancy, installing conferencing/telepresence systems and better protecting employees will likely be in high demand.

Air Travel

Current plans to provide bail-out funding for the airlines industry do not appear to address the core problem

of inadequate personal security and increased travel aggravation for passengers. This will likely be more obvious next year as the bail out fails to provide sustained protection for that industry. This realization may accelerate the development and sale of new plane designs that have enhanced security and data communications for the passengers. **Boeing** appears to be in better shape in this regard than **Airbus** because it has focused on a high-speed, low-capacity design rather than a low-speed, high-capacity design that travelers are increasingly likely to avoid. Near term, this industry will likely most benefit from new electronic employee authentication technology, and we expect efforts to shift from just trying to prop up the industry to dealing with the reasons customers are not flying in 2002. Passengers will likely not return to personal travel and business travel will continue to decline until personal security concerns are mitigated and the aggravation associated with such travel is brought back in line with the benefits. In addition, airlines will have to work on becoming more of a destination (something travelers look forward to) rather than something they would rather avoid. The longer the decline in travel goes on the more pronounced and permanent the shift to technologies that replace the need for such travel will be.

Electronic Security

Electronic attacks, including virus attacks, against individuals and corporations are likely to have increased sharply by mid-2002. While this will favor the firms that make a market in products that protect against these attacks, it will also increasingly place restrictions on what can be sent over e-mail and dramatically increase the need for better ways to authenticate users. This last component will be most pronounced for electronic commerce sites as identity thefts increase throughout the year, and attempts to disrupt or deface branded sites become more pronounced and better organized. Until this is addressed, aggressive business-to-consumer initiatives, like the one based on Microsoft's Passport, will likely stall in the market or represent an unacceptable exposure for the companies and people who use it. A national ID system, similar to the one proposed by **Oracle** CEO Larry Ellison, will probably be a requirement before any of these comprehensive e-commerce solutions can reach the same usage levels as automated teller machines (ATMs).

Personal Computers

Cost benefits that were driving centralized systems will give way to the need for redundancy and offline access. A reduction in network reliability associated with physical attacks will make the use of thin clients less attractive and may prematurely shift the trend back to stand-alone PCs with a few differences. These differences will include a constant background backup process, a much more robust virus-checking engine and a substantially improved (likely smart-card based) user authentication method. In addition, because instant messaging worked well during the disaster, this will become a feature that helps to drive the market once the messaging surrounding the PC is altered to address the related needs. Until these computers are repositioned around these concepts, sales will likely drop off sharply as people, and companies, shift buying behavior to more conservative products that directly address their need for higher security and communications.

Telematics

The need to know not only your location but the location of a loved one (and know that they could get help quickly if needed) will likely become the driving force behind telematics. Rental companies with this feature will likely be favored over those that don't have it. For families that travel or have children who are remote, in particular, the need for a locating-emergency product of some type will increase sharply in spurts with each attack on US soil. Initially driving this will be cars that approach the problem in a modular way so that the components can be either easily retrofitted or replaced as new technology comes along. Trusted brands like **Mercedes**, **Audi**, **Saab** and **Lexus** will likely enjoy an advantage as the technology and solution will best match with a trusted brand. (In other words, buyers will believe there is protection against premature obsolescence.) It is very likely that a personal mobile product that would also nest in the car will become popular at this time; however, like cell phones, it would have to be announced by a company that can both drive standards and is not seen as a competitor in the automotive market. This handheld implementation may be the most powerful as people realize that much of the time they are likely to need help will be when they

are away from their automobile.

Alternative View

This analysis is all predicated on the belief that the attacks on US soil will continue. Should that not be the case, the outcome will be decidedly different. Because habits are hard to break and people are resilient, if there are no additional large-scale US domestic attacks, it should take about six months for the buyers to gain a sense of security that allows them to return to the old habits. Some things, like the fear of air travel, may take longer for some, and even a six-month downturn in the travel market would be extremely painful. In addition, moves to reduce personal privacy and increase security would likely not be reversed, leaving many of the changes made during this six-month period in place.

On the other hand, if the expected attack takes place, things could get incredibly ugly for the US for a period of time, depending on the location and nature of the attack. Given the technology likely to be employed, the impact will likely be regional in nature, but would tend to make people distrustful of urban settings, ramp up urban violence sharply and substantially accelerate the initial moves to decentralize organizations and place them more aggressively in regional settings. Once again, smaller planes would be favored, almost to the exclusion of larger planes because of the nature and size of rural airports, and this too might favor the Boeing design. This scenario could dramatically fuel the telecommunications market as rural locations are forced to rapidly step up to urban requirements for networking and communications infrastructure, and emerging technologies like 802.11 wireless, two-way satellite data and voice over IP could see a dramatic boost as they could be deployed much more quickly than more traditional designs. Overall, the industry to watch would likely be biomed as much of the testing restrictions are short circuited to get defensive drugs on the market.

Findings

Two aspects of life in the United States will go through a great deal of change during the next 12 to 18 months. Travel will become vastly more restrictive and less popular and concerns about security over virtually all aspects of work and personal life will become a driving factor. Already gun sales are up in some areas sharply, and interest in general technology, personal and business travel and most luxury items has dropped just as sharply along with customer confidence. The perceived likelihood of another attack on US soil or on US citizens abroad is being increased by news coverage on exposures and government responses to those exposures.

At the time of this writing, *The Wall Street Journal* is reporting uneven and inadequate security in airports across the nation, and the government is proposing allowing commercial pilots to carry stun guns. In addition, during the last week, there have been reports of the potential for hazardous material trucks and crop dusting planes to be used as weapons of mass destruction, which points to just some of the sources of growing concern. It does appear increasingly likely that additional hostile events will take place on US soil, and any gains in consumer confidence will evaporate with those attacks. In addition, while no relation to the physical attack on the World Trade Center has been identified, one of the most damaging virus attacks has occurred during the same period of time, making it clear that the United States is both physically and electronically exposed. However, any response to this threat needs to be thoroughly considered, since it is likely that as one group of targets becomes protected others will be perceived as relatively vulnerable and this probably will not be missed by those that are taking these actions.

Recommendations

Security

The security function in the company needs to be responsive, comprehensive and coordinated. This means that physical site security and electronic security needs to be well coordinated and able to respond to an external threat quickly and effectively. Systems need to be integrated and based on technology and practices that effectively mitigate the realistic threats the company is facing. Ideally, the same system that provides

physical access to the site should be the system that also provides virtual access to the systems. Because of the clear exposure for identity theft, both a picture ID and a secondary, employee-specific identification method should be implemented. While a combination of biometrics and smart cards would likely be one of the better approaches, depending on the risk, a combination of picture ID and personal identification number (PIN) might be adequate for most instances. The focus on the system needs to be not only to provide secure access, but to have a clear audit and near-instant termination of access, both physical and virtual, if an exposure is identified. Clearly one of the first tasks should be to complete a full security assessment that would include both estimated exposure and readiness for the likely attacks that could occur to a company site or surrounding community. These assessments should include electronic, chemical, physical (including explosives and fire) and biological threats. Remember, even if the threat isn't local, if it occurs anywhere on the continent, executive management will likely want contingency plans in place at all locations. Having a plan could avoid mistakes that could cost lives and expose intellectual property.

Security should take an active role in training the employee population in how to identify, avoid and report potential threats. Clearly fire drills and safety audits should be increased during the time the threat remains in place.

Travel

Practices that avoid putting a working team on the same plane should be enforced, and all travel should be questioned, particularly if it involves sending a US citizen into potential threat. Employees traveling should be provided with communications; two-way pagers appeared to have worked best when phone lines were overwhelmed with disaster related traffic; however, cell phones did generally function during the actual attack. Current lists of cell phone numbers/pager addresses should be centrally maintained by human resources and, particularly for traveling employees, a hot line should be maintained (with at least one remote alternative) and supplied in case of an emergency. Traveling employees should have numbers for the local embassy (if traveling overseas), medical resources available to them and approved alternative transportation in case of a problem. In short, you should ensure the employee can call for help and/or quickly find a safe location in case of an exposure. A number should be available for family members to call if they believe their loved one is at risk. During a disaster, this number should be published on the corporate Web site.

Employees should also be cautioned to stay in relatively safe areas and travel in pairs, preferably with a local employee while traveling overseas. Overall, employees need to understand that their brain is their best defense against becoming a statistic or hostage, and staying away from questionable areas will have more to do with their safety than almost any other practice.

Vendors

Buyers, particularly in the US market, will be looking for solutions that address their security concerns. Certainly large global companies can respond by providing a mix of technology and consistent global localized services that local companies may not be able to match. Smaller firms should be better able to focus on the needs associated with companies or sites in close proximity to them. Overall, it is clear that if this conflict escalates, if the product doesn't have anything to do with making an individual or company feel more secure and safe, it likely will not meet sales expectations.

Travel Industry

This industry will be hit the hardest during this time. Its emphasis has to be on making the act of traveling appear safe to the traveler and something people look forward to rather than avoid. Current emphasis on arming cabin crews and eliminating meals actually may be counterproductive as it both adds to the apparent risk and makes the trip more tedious. If people are both afraid to travel and want to avoid the aggravation, giving them more travel in the form of frequent flyer points, particularly when they don't want to be away from home or can't afford the related vacation, won't mitigate the problem. Clearly the first target needs to be frequent flyers since they form the foundation for the industry. Travel clubs should be opened to these

travelers, and the costs associated with network and phone access, either while in the airport or on the plane, need to be substantially reduced or eliminated. More care should be taken to get to know them and to not only greet them by name when they arrive but be able to quickly provide information that could make their trip more enjoyable. A return to the practice of automatic upgrades to available business and first-class seats should be reinstated when there is room and the general focus of any marketing campaign should be on how well treated, secure and in-touch these travelers will be. If this is done effectively it should not only start pulling the frequent flyers back but provide a much stronger incentive to becoming one for the others that must travel.

Long term there should be an increased focus on smaller (more intimate), faster planes with some type of constant connectivity for the passengers. Over time, the airlines will need a much more comprehensive method to verify who a passenger is and what their unique wants and needs are so that they are in fact more secure, and therefore the airline can create a stronger relationship with their customers.

General

This is a time to think about programs like work-at-home (which, by their nature, are now considerably safer for large numbers of employees), the physical location of facilities in the Internet age and disaster preparedness (both professional and personal). We are entering a new age, and in this one, your mind is likely the strongest defensive weapon available. Use it.

References

Related Giga Research

Implications of the Terrorist Attack

[Anticipating the Long-Term Impact of the World Trade Center Attack](#), Rob Enderle

[Heightened Airport Security Affects Air Travelers](#), Steve Hunt

[World Trade Center Disaster: Tactical Response for Recovery](#), Colin Rankine

[Loss of Data From the World Trade Center Attack Is Dwarfed by the Loss of Knowledge](#), Keith Gile

Disaster Recovery Planning

[Disaster Recovery Planning in the B2B Arena](#), Ken Vollmer

[Virtual Server and Systems Management Technologies Will Play a Major Role in Future Disaster Recovery](#), David Mastrobattista

[Annualized Loss Exposure Calculations are Inadequate for Disaster Recovery Planning](#), Ken Vollmer

[History Still Comes on Paper — Safeguard Records With Imaging Systems](#), Daniel W. Rasmus

[Networked Contact Centers: Managing for Security and Outages](#), Elizabeth Herrell

[In the Wake of a Tragic Disaster: The Wrong Time to Make Business Continuity Investment Decisions](#), Colin Rankine

[World Trade Center Tragedy: Disaster Recovery Takes on Monumental Proportions](#), David Mastrobattista

[Collect the Right Data for Your Disaster Recovery Plan](#), Bob Zimmerman

[Getting Started With Disaster Recovery Planning](#), Colin Rankine

[What to Look for in a Business Continuity \(Disaster Recovery\) Manager](#), Colin Rankine

[Disaster Recovery Expectations in Outsourcing Agreements](#), Colin Rankine

[The Human Factor in Disaster Recovery Planning](#), Michael Grosvenor
[IBM's Business Continuity and Recovery Services: People or Product?](#) Michael Grosvenor
[Data Currency Affects Disaster Preparedness](#), Michael Grosvenor
[Disaster Recovery: Think Globally, Act Locally](#), Colin Rankine
[Disaster Recovery: Hot-Site Selection](#), Colin Rankine
[Selecting a Disaster Recovery Service](#), Michael Adams
[Disaster Recovery Program Costing: The Missing Element](#), Will Cappelli
[The High Price of Disaster Recovery Services](#), Will Cappelli
[Disaster Recovery: To Outsource or Not to Outsource](#), Colin Rankine

Security

[Stay Alert for Viruses in the Aftermath of Attacks](#), Jan Sundgren
[Protecting Your Organization From Potential Terrorist Activity on the Internet](#), Michael Rasmussen
[Best Practices in Security: Bomb Threats](#), Steve Hunt

Capacity Planning/Redundancy

[Emergency Telecoms: Wireless Data Is More Reliable Than Voice](#), Brownlee Thomas
[Business-Critical Internet Applications: Addressing the Requirements Capacity and Business Continuity](#), Joel Yaffe
[Common Sources of Failure in Router-Based WANs](#), Lisa Pierce
[Access Redundancy Is Essential for Communications-Dependent Organizations](#), Lisa Pierce

Management Issues

[Video Conferencing Best Practices](#), Daniel W. Rasmus
[Outsourcing to India: Still A Viable Option After Terrorist Attack](#), Stephanie Moore
[Now Is Not the Time to Stop Learning: Incorporating Lessons Learned Into Disaster Recovery](#), Daniel W. Rasmus
[Leadership Styles Reflect Roles in Disaster Response](#), Robert Klehm
[Virtual Communities Backup Traditional News Sources](#), Daniel W. Rasmus
[Operating During Crisis: Recommendations for Call Centers, Technical Support and Help Desks](#), John Ragsdale
[Employee Data Is Critical in an Emergency](#), Paul Hamerman
[The Pillars of Emergency Preparation](#), Steve Hunt
[Modifying Corporate Privacy Policies in the Interest of National Security](#), Steve Hunt
[The Challenges of Managing Geographically Distributed Organizations](#), Marc Cecere and Mark Rosenberg
[Collaboration Environments](#), Daniel W. Rasmus