Points of Defense

A study into different industry sectors' propensity to mail-based security attacks

A Pitney Bowes Management Services Report

Management Summary, May 2006

Key Findings

- Organizations are increasingly recognizing the importance of protecting themselves and their employees from terrorist attack.

- The advent of extreme terrorism or activism - where anarchic disruption is the aim and restraint in the use of toxic agents has disappeared - makes it doubly important for organizations to take defensive measures.

- The costs of closing down a contaminated facility, temporarily recreating it elsewhere, and then restoring it to normal, have been seen to cost many millions.

- The mailstream is a point of vulnerability which attackers have increasingly taken advantage of, whether for explosive, chemical or biological agents.

- Equally, the mailroom is one point of entry where it is possible to fully monitor and manage processes so that threats are identified and neutralized, or at least contained.

- The government (+155% over average), finance/banking (+137%) and high-tech (+91%) sectors are most subject to the receipt of suspicious letters and packages. This is probably because terrorists often see these sectors as potent symbols of Western capitalism. Moreover, government is responsible for the formulation of sometimes-unpopular policies.

Introduction

The clear and present danger of terrorist attacks in the US and Western Europe has been vividly demonstrated by the well-known outrages experienced in New York, Madrid and London. For the US, the shock of suffering the first major act of foreign terrorism on home soil has fundamentally altered the country's view of global political policy. In Spain and Britain, both countries that have had to deal with sustained internal terrorism over many decades, the effect on national psyche has been somewhat less radical.

However, the new face of terrorism has a particularly frightening aspect – that of pure anarchy. Commentators on the subject have noted that the activities of the IRA and ETA – whilst unacceptable in democratic society – nevertheless had political objectives. In addition, those objectives served to limit the level of pure damage to civil society that its proponents were prepared to perpetrate. Secession and political power were the endgame. In contrast, anarchy – or the disruption and destruction of the structure of Western civil administrations as an end in itself – is the aim of the new breed of terrorist.

This motivation brings with it a rising of any barriers to the means of terrorism. Any means, however 'dirty', may be used to achieve the terrorist's objective, spanning explosives to chemical and biological agents.

Certainly, these dramatic assaults have served to heighten the awareness of the public, of governments and of the business community to the issue of security, leading to the institution of measures to protect people, politicians, public servants, businesses and property alike. Yet such attacks are also those against which fewest measures can be taken, so wide are their possibilities and so unpredictable are their sources. Therefore, organizations have had to concentrate on addressing the points of potential attack that *can* be monitored and practically controlled.

Most media attention naturally tends to be focused on major terrorist outrages or campaigns. However, for organizations seeking to protect themselves, their employees, their property and their finances, the accumulation of smaller and far less publicized threats actually poses far higher total risk than major acts of terrorism. These individual threats range across the actions of disgruntled employees, activist groups and straightforward criminality. A review of attacks in the UK and US last year offers many examples, a selection of which includes:-

- Packages containing white powder or incendiary devices received by addresses in the are of Luton, UK[1]
- The threat of attack specifically on pharmaceuticals company Glaxo by animal rights extremists[2]

---

[1] Source: Communications Workers Union, http://www.cwu.org/default.asp?Step=4&pid=508

- A hoax powder threat sent to UK Prime Minister Tony Blair[3]
- Closure of the UK Passport Office because of powder received in letters
- The order by a judge in Greensboro, North Carolina, that a man who sent bomb threats should repay the cost of temporary closure to the businesses targeted
- A 19 year jail sentence for a Philadelphia religious fanatic who targeted abortion clinics with fake anthrax letters[4]
- Powder sent to employees of British automotive information company HPI[5]
- Mail threats and a bomb scare at British TV's Big Brother house[6]
- Letters containing powder causing an evacuation at IBM
- Anthrax scare at the UK Labor Party's office and, on a different date, a similar incident at Conservative Party headquarters[7]
- Animal rights extremists opening a violent campaign against BAA, the company that runs most of Britain's big airports, for its role in importing live animals for laboratory research[8]
- A bomb attack on HSBC in Istanbul[9]

Mailstream as the Point of Attack

One of the main interfaces with an organization is the mail it receives every day. The ease with which a terrorist, a disgruntled customer, an activist group or a criminal can introduce threats to a company or government organization in the guise of an envelope or package means that the mailstream and the mailroom are critical points of vulnerability. At the same time, the mailroom can also be made into a highly controlled environment where mail is screened, threats identified and danger isolated or averted.

If a larger organization is either attacked or contaminated, the cost of even temporary closure and relocation can be enormous. In 2002, the largest of the U.S. Senate's office buildings shut down for more than three months because of anthrax contamination. Decontamination

---

[2] Source: The Times, http://www.timesonline.co.uk/article/0,,2-1800729,00.html

[3] Source, Yahoo, http://uk.news.yahoo.com/15062006/325/woman-72-charged-blair-powder-hoax.html

[4] Source: Kaiser Foundation, http://www.kaisernetwork.org/daily_reports/rep_repro_recent_reports.cfm?dr_cat=2&show=yes&dr_DateTime=07-11-05

[5] Source: BBC, http://news.bbc.co.uk/go/rss/-/1/hi/england/wiltshire/4600279.stm

[6] Source: BBC, http://news.bbc.co.uk/1/hi/entertainment/tv_and_radio/4614593.stm

[7] Source, Cambridge Evening News, http://www.mailroomsafety.us/mailroomsafetynews/newsarchives.html

[8] Source: The Guardian, http://www.guardian.co.uk/animalrights/story/0,,1494462,00.html

[9] Source: CNN, http://www-cgi.cnn.com/2003/WORLD/europe/11/20/turkey.blast/

at the Hart Office Building[10], which houses the offices of 50 of the 100 senators and their staffs, was estimated to have cost over $30 million. In order to deal effectively with the threat of 'dirty' attacks in the UK, the Government Decontamination Service was established as an executive agency within the DEFRA family on 1 October 2005. Establishment of the GDS is part of the much wider CBRN Resilience Program, led by the Home Office, which is ensuring that the UK is capable of responding quickly and effectively to deal with and recover from the consequences of CBRN incidents, particularly those caused by terrorism.

At the same time, larger private and public sector organizations have been establishing secure mailroom operations, often at remote sites, usually operated by third party specialists. Government operations in both the US and the UK operate remote facilities of this sort. The facilities protect government officials and representatives, but also have to operate to service standards that ensure genuine messages reach their addressees in a timely fashion.

The volumes of mail received by larger organizations in the US and UK, which require security screening, are enormous. In the US, these organizations receive over 20 billion mail items per year in roughly equal proportions from households or from other businesses. In the UK, the volumes received by larger businesses and government organizations are around 3.3 billion mail items per year.

Research Findings

What, then, are the sectors that receive most suspicious packages? Which industries are most at risk and most in need of a secure mail facility? In order to give a broad-brush initial answer to this question, Pitney Bowes Management Services analyzed a representative sample of organizations in the US and the UK where such facilities exist. Using a year's worth of data on mail throughput and suspicious package investigation, an index of vulnerability was constructed amongst key sectors, revealing relative levels of suspicious letter or package receipt.

The resulting index figures showed that government, finance and high-tech companies stand out as those mainly at risk from attack through the mailstream – a scale leap ahead of any other sector studied.

As the formulator and issuer of legislation, policy and taxation, as well as sometimes-controversial foreign policy, government organizations are seen as the principal target for extremists and anarchists alike. Nor should we forget the occasional outbreak of civil disobedience, which characterized the British populace's outburst against the Poll Tax in the 1980s. Internal terrorism in Great Britain has included audacious attempts on the heart of

---

[10] Source: CNN, http://transcripts.cnn.com/TRANSCRIPTS/0201/16/bn.03.html

government itself, notably the rocket launches on Whitehall and MI6. Alongside these attacks, however, there was a steady stream of letter bombs directed at individuals, government departments, police and companies. In the US, the Senate, the House of Representatives and the Pentagon have been the main targets of the 2001-2 Anthrax campaign.

Next in line as prime targets are finance and banking organizations. Famously under attack in New York on 11th September 2001, financial institutions are most frequently selected by foreign and homegrown terrorists as symbols of what they wish to attack in Western society. We have but to think of the World Trade Center in New York or the Baltic Exchange in London. This means that financial institutions have to take particularly careful mailroom security precautions. Both the World Bank and the International Monetary Fund have been targeted with anthrax in the mailstream. The European Central Bank was targeted with letter bombs in 2003. Additionally, the risk and losses associated with even a temporary shutdown are arguably much more expensive in the financial world – particularly for capital markets institutions who are dealing with huge sums and often-complex instruments on an hourly basis.

Third in our index of vulnerability to attack through the mail comes the high-tech industry. Again, we believe that this is the result of hi-tech being perceived as a recent and prominent characteristic of post-millennial Western society. Hi-tech companies are perceived by individual and organized terrorists, anarchists and criminals to be an essential pillar of society, capitalism, economy and government, and so their disruption will be seen as fundamentally destabilizing. Moreover, the hi-tech sector also numbers amongst its members such natural targets as surveillance technology companies and defense industry players.

Conclusion

In summary, none of the sectors studied, even if their vulnerability score is below average, should be complacent. For instance, although the pharmaceutical industry sits at 47% below average, this is not a comprehensive view of company risk mailstream-based attack, as we know that animal rights activists tend to target employees in their own homes. In another example, the risk of attack through the mailstream for insurance companies – at 8% below average – usually emanates from policy holders whose claims have not been satisfied, and so these companies face a deep-rooted threat which needs to be addressed at a causal level bound up with the way the company does business in the first place, rather than simply providing a protective filter to screen unexpected dangers. However, it remains evident that government, finance and high-tech organizations that do not yet have secure facilities screening their mail need to act fast if they are not to face insupportable levels of risk.

Appendix – Secure Mail Measures

A variety of measures techniques and technologies are employed in secure mail centers to identify, investigate and deal with suspicious mail. They include:-

- X-ray
- Sealed areas
- Sealed protective clothing
- Biological agent detectors
- Poison detectors
- Negative pressure rooms
- Vacuum cleaning
- Irradiation
- Video surveillance
- Robotic investigation
- Trained animal detection

Staff is also trained in the detection of suspicious packages. Typical tell-tale signs include:-

- Restrictive markings (such as “private and personal”)
- Lack of return address
- Excessive taping
- Home-made labels
- Attempts to avoid investigation (such as “do not x-ray”)
- Addressed to job function only
- Stains, discoloration, crystallization
- Unusual odors

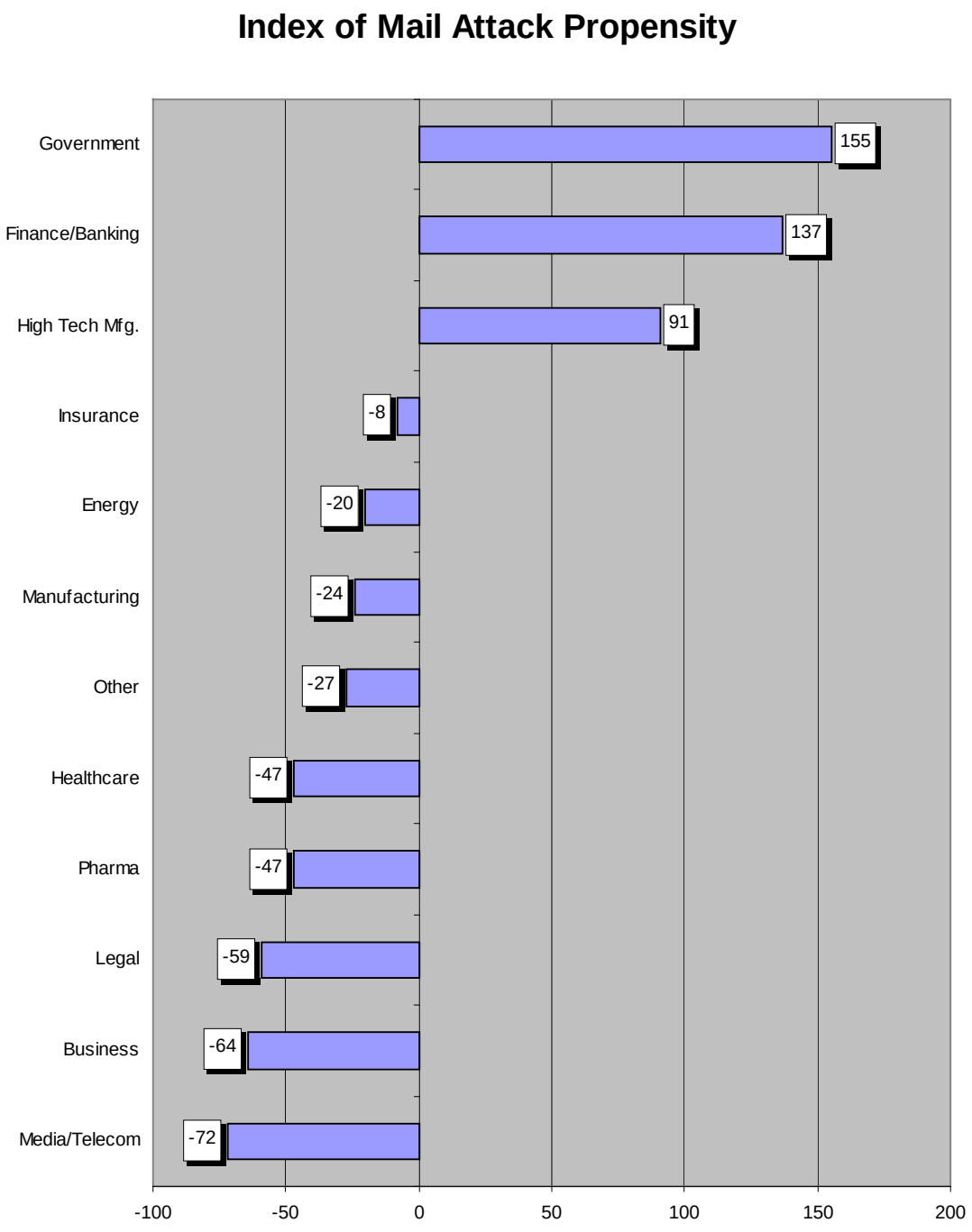
Finally, a new development is now being implemented amongst a number of pioneer organizations in the public and private sectors. The notion of digital mail provides an important interface between external mail and internal computer networks, while at the same time providing an impenetrable security layer. Incoming mail is opened and scanned in the remote or isolated mailroom. The recipient is then sent their mail electronically, completely obviating any physical threat – explosive, chemical or biological. At the same time, the company or government organization obtains the advantage of being able to archive all mail electronically and then make it easily retrievable – for customer service, research, knowledge sharing, compliance and a host of other uses all of which contribute to efficiency and/or competitive edge. We expect to see substantial growth in the adoption of digital mail over the next five years.

Appendix – Methodology

Pitney Bowes Management Services serves a wide and representative range of over 1,200 large private and public sector organization in the US and the UK, delivered through 75 service centers. This sample represents approximately 9% of the 14,000 large companies in the US and UK – defined as those with over 500 employees.

This study examined the occurrence of suspicious packages/letters being identified over the last year. The resulting statistics were turned into an index – to preserve corporate anonymity – and then the identification rates compared across different industries.

Charts


Index of Mail Attack Propensity
Government
Finance/Banking
High Tech Mfg.
Insurance
Energy
Manufacturing
Other
Healthcare
Pharma
Legal
Business
Media/Telecom
155
137
91
-8
-20
-24
-27
-47
-47
-59
-64
-72
-100
-50
0
50
100
150
200