



2006 Attack Trends Report & 2007–2008 Crystal Ball Forecast

Doug Howard
COO, BT Counterpane

Bruce Schneier
CTO, BT Counterpane

Table of Contents

INTRODUCTION	3
MAJOR TRENDS	3
EMERGING TRENDS	5
SAMPLE DATA: WHERE OUR PROJECTIONS ORIGINATE	10
CONCLUSION	11

INTRODUCTION

Since 2004, the BT Counterpane Attack Trends Report has been the leading source for trends in network attacks, both for analyzing their impact on businesses and forecasting risk. This year's report is a review of data from January 2006 through February 2007. It discusses two major areas of concern, and highlights nine trends that will have a significant impact on both the development of the security services industry and every business that uses the Internet.

MAJOR TRENDS

Cybercrime

The first major trend is the continuing rise of cybercrime. In 2006, hacking and cyber attacks have continued to transform from a hobbyist activity into a criminal act. We first reported on this trend in 2005, and it has continued. Although the majority of network security events are still low-tech hobbyist activities that are not criminally motivated, the level of criminal activity continues to grow at a significant rate, and now represents the highest risk to enterprises and internet users.

While hobbyist attackers keep individuals and enterprises busy fixing largely superficial concerns, such as defaced web pages, low-impact worms, and the effects of denial-of-service attacks against networks, criminal attacks are more dangerous and more damaging because they are motivated by profit. Over the past two years—and especially in the last 12 months—we estimate, based on real-world experience, that financially motivated criminal attacks have risen fivefold and have resulted in the loss of millions of data records worldwide relating to individuals, hundreds of million of dollars in direct financial losses, and many billions more in indirect losses in areas such as reputation and remediation.

On the surface, this may seem contrary to market reports such as "2006 CSI/FBI Computer Crime and Security Survey" and other industry reports; however, if you read the details closely, primarily sampling of trends revolve around virus and Trojan activities. The statistics around focused attacks, such as DOS/DDOS, system compromises, system compromise, and sabotage have historically rarely been captured, and are more often unmeasured from a financial perspective. As such, the "gut estimates" from respondents are based mostly on what they impressions, than on hard statistics.. More and more, the feedback is based on tracked metrics within enterprises. With a current lull in the industry of major worms and Trojans, this emotional sense of security is further compounded.

Criminals versus Hobbyists

Criminals differ from hobbyists in several respects. First, criminal attackers care less about style. Hobbyist hackers look for new and clever attacks, while criminals will use whatever works. Second, hobbyists regularly advertise their presence, while criminals are more likely to be stealthy. Third, hobbyists generally don't discriminate among who they attack, while criminals are more likely to target specific organizations. Finally, criminal attackers are less risk-averse; they're willing to risk jail, which hobbyists are largely not. As such, criminal attackers will engage in behavior that hobbyists avoid, will use higher-quality exploit code, and are less likely to be noticed by their victims.

Typically, specific industry verticals are targeted by criminals based on the following criteria:

1. The perceived value of the target

While corporate trade secrets are an occasional target, the primary target of choice is credit card information and personal data that can be used to commit identity theft.

2. Ease of gaining access to a target or acquiring the information

Successful bank robbers do not blindly walk into a bank and attempt to rob it. Instead, they scope out several potential targets and determine which one provides the greatest opportunity for success. Successful hackers are much the same. They will scope industries, companies, and even security technologies, to determine the path of least resistance.

3. Risk level of being caught

Stealing a highly classified military jet and delivering it to a rogue state could probably secure a thief a lifetime retirement, but the likelihood of getting caught is far too great. Better to steal plans of the aircraft and a few key components than to act in such an obvious fashion. Information assets are often targeted simply because they're easier to steal, and can be stolen from the safety of the criminal's own country.

BT Counterpane's monitoring data, representing hundreds of networks around the world, illustrates this trend toward the criminalization of hacking. We continue to see a decline in the "noisy" brute-force vulnerability scanning that hobbyist attackers tend to favor, and a corresponding increase in targeted, stealthy, and sophisticated scanning. We continue to see an increase in the sophistication of automatic worms. Today's most sophisticated worms are slower and stealthier. They are deliberately engineered to better evade anti-virus software, and spread slower to remain undetected by those companies longer. They

sometimes engage in sophisticated reconnaissance before attacking their targets, or limit their spreading to particular predefined targets. We also see more variants on successful worms—Netsky is a good example—demonstrating the criminal tendency to stick with successful techniques rather than the hacker tendency to invent something new.

Businesses in the financial sector are frequent targets. Many attacks against financial institutions are initiated by IP addresses in Romania, and Romania is one of the best-known locations for organized crime operations.

Industry Consolidation

The second trend is continued consolidation in the managed security services sector. The trend toward consolidation is driven by customers' need for tools and services that allow for a holistic view of their business. While point solutions for security, compliance, network health, and other areas continue to gain traction in the marketplace—and new products generally come from startups—successful niche companies are often acquired by larger IT services companies. This allows these point solutions to become part of an integrated offering that gives the customer a single console, or portal, for viewing a broad range of activities.

If the ingenuity of the pure-play product or service is not lost, then acquisition is a good thing. Even Counterpane was acquired in 2006 by BT to layer the event collection and correlation technology across its broader base of service offerings. In addition, the BT Counterpane service was integrated with BT's Risk Cockpit (a risk assessment solution) and Network Health monitoring, so that customers have the option to view their enterprise from desktop to application. This integration provides risk analysis, compliance, network health, and security viewpoint from one provider.

Industry analysts covering the managed security services sector agree that the trend toward security service outsourcing will continue in the future. At the RSA Conference in February 2007, for example, a major theme was that enterprises are becoming less and less concerned with the underlying technologies of security and more focused on retaining a trusted security provider to make those decisions for them.

EMERGING TRENDS

While the two major indicators above frame our discussion, it is equally important to examine emerging trends, as they will form the basis of activity, discussion, and decision making in the coming year.

The Convergence of Physical Security and Network Security

Look into the future and what do you see? Employee ID cards that tracks location, activities, and access. From a corporate security perspective, keeping tabs on personnel

and limiting their ability to perform functions based on location is an attractive option. We anticipate that while physical and network security will continue to be managed from two separate domains for the next three to seven years, early adopters of new technology will begin moving to a combined security structure and process.

The Increasing Importance of Correlation

Within the IT industry, correlation is defined very loosely. One definition is that correlation is taking several diverse elements of information, and combining them in order to draw a higher-value conclusion.

In more tactical terms, correlation is a means to increase the accuracy of any security product or service. It is used to determine when a sequence of events is an attack and not a false alarm, or that an abnormal event occurred and is not simply an abnormality in the security system. Used properly, correlation tools can be used to determine when an incident should be escalated to a higher-value automated analysis system, or to a human. Without correlation, an IT department would be overwhelmed by the tens of millions of events occurring on an average network each day.

As event data volumes increase, improved correlation must follow. We predict that more and more security products and services will offer correlation features, and that different products and services will improve their capabilities to correlate data between each other.

The Rise of End-to-End Security

End-to-end security, implemented with a layered approach, is the most effective way to deploy security, and we predict a rise in this security approach.

However, there are two real-world issues to consider. First, it introduces complexity in deployment. Second, it introduces capital expenses and operational expenses. It might be more secure to deploy a security-enhanced router, a double layer of firewalls plus a higher layer port layer firewall, combined with a double layer of IPS, plus an application-specific firewall and a host-based IPS, but the result is an expensive, difficult to manage, multi-vendor solution.

If properly deployed in today's environment, endpoint security can often, although not always, provide better value than a firewall. Certainly we wouldn't recommend not having a firewall or IPS. However, in normal environments these technologies provide little to no protection against internal attacks, which represent a large proportion of financially damaging events that occur today.

With consolidation in the marketplace and the continued successes of managed security firms, more cost-effective end-to-end solutions will be introduced into the marketplace.

Are There Bad Countries, or just Bad People?

China, Romania, and North Korea are often cited as the countries of origin for today's most damaging attacks. The majority of the attackers based in these countries are not government-sponsored. Instead, the hackers choose to set up operations in these countries because they provide a lack of structure in terms of identifying, tracking, and prosecuting offenders. This is no different from any other area of crime, where criminals find ways around established laws by exploiting locations where they know the risk of prosecution is low.

While the CIA began making this distinction between bad people and bad countries in many of its reports from the 1980s, it is only now gaining traction in the IT sector and in cyber crime prosecution.

The Need for Clear Policy: Defining Unauthorized Use and Unauthorized Access

Most enterprises do not distinguish between unauthorized use and unauthorized access. However, it's an important difference. Unauthorized use is typically defined as when a user, not necessarily an employee, performs activities on an enterprise resource that would not be approved within the enterprise's acceptable use policy. Unauthorized access is when a user, potentially an employee, gains access to a system that a business would not have allowed within its security policy.

In either scenario, the user may not be acting maliciously or intentionally bypassing security efforts. Instead, the user may have effected some sequence of events that resulted in the user being able to perform an activity that, if the business knew of the activity, would not approve.

A common unauthorized use scenario is where employees use the corporate network for peer-to-peer activities, such as file sharing. A common unauthorized access scenario is where an employee, such as a salesperson, has access to all customer data, as opposed to just his territory's accounts.

While the distinction between the two seems clear, the failure to make it is a common occurrence. This, in turn, leads to unclear security policies that cannot be supported properly at the operational level. With new ISO standards and definitions being introduced into the marketplace that provide more tactical recommendations, as well as vendors that tie reports back to common compliancy themes, we believe that enterprises will have a better view of what policies are effective and which ones are only provided lip service as we roll into 2008.

A Misspent Youth: Why Businesses Won't Be Hiring Reformed Hackers

Because of government contracts, most large service providers are prevented from hiring personnel with criminal backgrounds. Additionally, many other corporations have internal rules that do not allow the hiring of personnel with criminal histories. While most individuals believe that a person can be reformed, and that things a 16-year-old does shouldn't be held against him for his entire life, the unfortunate fact is they often are in the real world. The "2006 CSI/FBI Computer Crime and Security Survey" reported 86% of 606 respondents would not consider hiring a reformed hacker.

In other words, with the increasing criminalization of hacking, and improved ability and willingness to track and prosecute even hobbyist activities, what a 16-year-old does may have a significant impact on his future plans. As the Information Security industry continues to mature, we predict that standards for employment will become much tougher and background checks more stringent. While not all companies require a Department of Justice or Federal background check prior to employment, as BT Counterpane does, there will definitely be greater scrutiny and formalization of employment practices and standards.

A New Policy in the Portfolio: Do You Have Cyber Insurance?

The "2006 CSI/FBI Computer Crime and Security Survey" identified 29% of 571 respondents as carrying some form of external insurance policy to manage their cyber security risk. While these policies exist, they can be very hard to understand and compare for several reasons. There are significant differences in the ways policies define security baselines and measure losses due to security breaches. This leads to policies with defined exceptions and wildly varying rates, and the result is that the buyer is often uncertain how competitive his policy is and how much it reduces his overall risk.

However, despite these uncertainties, we believe that we will see more corporations investing in cyber insurance policies, simply because they are offered. Once the leaders in each vertical have bought cyber insurance policies, there will be what amounts to industry peer pressure to comply. Inevitably, a few companies will begin to use it as a marketing tool to reassure increasingly skeptical consumers, and the moment this happens, it will no longer be an optional extra.

Recalculating Security as a Cost of Doing Business

There are many different ways in which organizations try to measure the value they receive from their security expenditures. Return on Investment (ROI), Investment Rate of Return (IRR), Total Cost of Ownership (TCO), and Net Present Value (NPV) all provide value in their own scenario.

These different measurements have been driven by the ongoing struggle for enterprises to justify security expenditures. But while it is possible to demonstrate how security will

improve revenue through standard ROI, IRR, TCO, and NPV calculations, this rarely results in good math.

A more effective approach is to recognize that security investment, like business continuity and disaster recovery investments, over time provide competitive values but rarely can be measured in realistic dollar amounts. Rather than attempting to justify security as part of the bottom line, this approach recognizes that security expenditures are cost of doing business through risk reduction. We predict that more organizations will take this attitude in the future.

The Increased Impact of Social Networks on Security

Peer-to-peer communications—that is, the creation of an insecure communications link between two users or a group of users—allows for chat, file sharing, and other activities born of the Internet age. Often these communication paths bypass established security practices, such as firewalls, IDS/IPS, personal firewalls, and gateway AV systems. In particular, social networks introduce two primary security problems:

1. They create a conduit from the member to the social environment (i.e., the actual servers that provide the connection point between members of the social network) that often creates an unprotected path of peer-to-peer communications.
2. They introduce the risk of perceived familiarity with another individual. While each party may believe he or she knows the other individual based on the information shared, and willingly provides additional information, the reality is that very little is truly known about the person on the other end of the forum, chat room, or IM.

Since the first virtual social networks were created, there have always been people who misrepresent themselves to gain competitive information or to furnish false information in the pursuit of competitive advantage. In social networks, this comfort with another individual is taken further as relationships are created over time and natural defense and suspicion is reduced. This could result in the release of proprietary information (customers, strategy, financials, and planning) to someone perceived to be a friend. While this behavior is all harmless if the person, or people, in the network don't use the information to their advantage, the possibility for exploitation is always present.

Currently, a majority of enterprises do not allow, or have defined acceptable use policies, for peer-to-peer communications on their corporate environments. However, these policies are a just that— a written policy that is documented practice and which relies on self enforcement, rather than an inability to access constrained by an enforceable technological restriction and violation reporting. We predict in the coming year that there will be more technical controls along these lines, and that as more enterprises are compromised due to peer-to-peer activities, more enterprises will tighten their acceptable use policies.

SAMPLE DATA: WHERE OUR PROJECTIONS ORIGINATE

BT Counterpane currently monitors data from over 550 customer networks. When combined with BT and the new solutions being deployed that leverage the BT global infrastructure, we monitor over 200,000 endpoints. Our largest security customers have in excess of 5,000 devices each under management and, like BT, have global footprints. Our services are not limited to the Global 1000; rather, they provide value at an individual consumer level, for small- and medium-sized businesses alike.

Our sample data and experience encompasses all major industries, and in most industries we have three of the top ten companies in each vertical. Specifically, our data encompasses Financial Services (including Banking, Brokers, and Insurance), Government (Federal and State), Airline/Travel/Hospitality, Healthcare, Pharma, Religion/Non-Profit, Energy & Utilities, Manufacturing, Education, Retail and Consumer Goods, Telecom/Computer Services, Book Publishing, Automotive & Transport, Agriculture, and Business Services. Because industry sample size, number of devices per customer, and location of device could skew the statistics, BT Counterpane has normalized the data by applying averaging to various categories of the data. This allows each device to carry an equal weight, regardless of number of devices within a specific customer and associated industry.

While the amount of raw event data generated is certainly a trendable and statistically relevant piece of information, it's not the data that customers deal with each day. Rather, what events a customer must take action on carry a much higher priority. While Financial Services generate more raw events, Retail/Consumer Goods and Healthcare generate far more actionable events. Normalized for false positive contributions, these two industries still generate proportionately more offensive actions from both internal and external sources. Approximately 65% of all events that break policy originate from within the enterprise environment.

Another focus that helps us forecast activities within verticals is the amount of probing that occurs within an industry. Unlike scanning, which doesn't generally attempt to find one particular weakness, but only the general posture, probing tends to take the next step and test the weaknesses discovered during a scan. Historically, the level of probing activity an industry is subjected to generally foreshadows the number of actual penetrations in the following year.

CONCLUSION

What Does it All Mean?

Fortunately for us that have careers in security, the complexities and rate of change for technologies is not slowing; threats continue to evolve and risk continue to increase. However, we, as security professionals, must continue to juggle budgets, resources and priorities.

While the security industry and associated best practices in policy, compliance, standards and automation may be maturing, it's still far from mature. However, C-level, executives, and leaders of enterprises, service providers, and product manufacturers have all realized that security is not an enhancement that might simply provide a competitive advantage; rather, security is a necessity of doing business. The challenge these leaders are currently facing is how to prioritize projects to the highest-impact activities are allowed to bring the greatest value to an organization. This starts with recognizing the business drivers, areas of weaknesses, and highest risks within each unique enterprise.