Building a Business Case for Computer Forensics

Kelly J. (KJ) Kuchta, CPP

A client's recent experience with a mysterious and unexpected crash of its servers demonstrates the value of having good information. The crash caused the loss of data to that client's critical Accounts Payable and Accounts Receivable records that kept its banker informed of the company's financial state. After making an initial assessment of the issue, the company inquired about the use of computer forensic services to identify the source and come up with a remedy. A week after pursuing answers through some of its product vendors produced a lot of frustration and no answers, the services of a computer forensic professional were requested. On day one, the forensic expert identified the potential source. Day two produced a confirmation of what was suspected on day one. By the end of day three, the company was back to business as usual. All of this was possible because information about the incident was available.

In a previous issue, I pointed out that computers capture large amounts of information. Deleted files, revisions, and information about user activities are readily available to a computer forensic professional. Today, almost every piece of paper with information on it is or was in a digital format at one time. Events that occur on or over the computer hold key pieces of information vital in answering the what, who, when, where, and how of a particular issue. Unfortunately, most of this information is not found in plain view. Technology is every malcontent's dream come true. It provides anonymity and allows malicious individuals to perform their actions from remote places.

Are you swimming in information? If you answered "yes," is it the right kind of information? Often, the key ingredient that makes information systems valuable is having good information. Having the right quality and quantity of information makes decisions timely, effective, and result oriented. Inquiring about a com-

KELLY J. KUCHTA, CPP, is an area leader for Ernst & Young's computer Forensics Services Group in Phoenix, Arizona. He is an active member of the High Technology Crime Investigation Association (HTCIA), Association of Certified Fraud Examiners (ACFE), Computer Security Institute (CSI), International Association of Financial Crime Investigators Association (IAFCI), and the American Society of Industrial Security (ASIS). He currently serves as Chair of the ASIS Standing Committee of Computer Security.

puter forensic engagement, many clients often ask, "How much will it cost and how do I know it's worth it?" With a high degree of accuracy, I can estimate cost based on the scope of the work. Clients must, however, consider the question, "How much will it cost me by *not* having the information?" After a reasonable answer to this question has been found, we can determine how much it will cost. I highly recommend that forensic professionals answer these questions to determine whether the client will be satisfied at the end of the engagement.

My initial rule of thumb is that if the expense of getting the information is greater than the cost of *not* having the information, the chance of success, as measured by client satisfaction, is doubtful. It sounds obvious, but many clients fail to consider this fact. Next, I ask them to determine the value of having the right information, and I give them the probability of success. When calculated together it provides an estimate of the value they can expect for their effort. The first test is to determine the breakeven point; anything above that is gravy. There are certain times (e.g., when responding to regulatory issues) when you will have to spend the money regardless of the breakeven point.

Don't forget to measure the loss of consumer or business partner confidence and goodwill in determining the cost of not having the information. Goodwill is a legitimate asset. In the financial statements of most major corporations, particularly during mergers and acquisitions, "goodwill" is accounted for as an asset. I like to use a two-question test for the skeptics. First, how would your customers react if Mike Wallace aired this issue on *Sixty Minutes*? Second, what would Wall Street's reaction be if the story appeared on the front page of *The Wall Street Journal*?

Computer forensics has not been a tool used with any frequency in the past by corporate America. However, as business becomes automated and technologically sophisticated, these tools ought to be available. Once you have made the decision to put computer forensics in your toolbox, you need to decide whether you are going to buy it, or rent it when needed. Before you make that decision, though, it's helpful to understand what you are buying and how it will perform. Let's walk through your options in building it internally (buying), finding an outside resource (renting), or using some combination of the two. There is no answer that will work for everyone. There are a number of business considerations that need to be evaluated. These are discussed in the following sections.

New technology has a tendency to increase security risk until the "bugs" and "process" have been ironed out.

NUMBER OF INCIDENTS

A good starting point in determining the number of incidents that you might encounter will be found in your historical experience. Using this baseline, consider changes in technology, growth rates of your business, and, finally, trends in employee misconduct and network intrusions. These considerations will change your baseline number to a more realistic mark. A company that is migrating to E-commerce or using technology as an enabler for either its employees or customers has taken on a higher risk. Technology provides opportunity and easy access to the soft underside of your organization. New technology has a tendency to increase security risk until the "bugs" and "process" have been ironed out; there will be bumps in the road until the technology has matured.

Today's companies rarely have time to conduct field tests on changes because of earnings pressure from Wall Street and the drive to be first to market with new products. The corporate mentality of "we're in the business to make money, not test products" leads to cutting corners on security. My experience has shown that a company experiencing a high growth rate is vulnerable to fraud and other events that cause economic loss. During periods of growth, it is often difficult to hire and retain a large number of good people. Organizations have a tendency to become less selective in their hiring policies during these periods. Or even worse, they will use a temporary workforce that does not go

through the selection process and has no loyalty to the organization. I experienced this in a situation in which a client's temporary employee was able to commit a large fraud within a week of being on the job. The technology and business practices used to further the growth rate of the organization became its Achilles' heel.

Just as companies have realized that technology is an enabler, so have the predators of the world. Fraudsters, hackers, and snoops all use the computer as a tool to carry out their mission. Crime rates show that the computer is increasingly involved in crimes. This trend will continue to rise, and corporate America needs to consider it in their security program.

COSTS

Comparing the costs associated with having an internal computer forensic resource vs. hiring outside resources involves many components. The geographic locations of the work, the cost of acquiring forensic equipment, and having trained personnel to complete the work are a few of the considerations to be explored in greater detail.

The locations where computer events might occur will dictate the cost and the ability to respond to these situations. This is particularly true if some of the locations are overseas. In addition to travel expenses, consideration of cultural, governmental, and response times must be evaluated, such as: Can the computer forensic professionals stop what they are doing and respond on short notice? Do they speak the language? Do they have passports and can they get work permits?

The people cost is always the larger portion of most business costs. The usual human resource expenses such as benefits and insurance should be expected. What might not be expected is the average salary of an experienced computer forensic professional. The profession is a relatively new one, with most experienced professionals coming from law enforcement and the military. Salaries in the $60,000 to $80,000 range are not uncommon. Because most are gainfully employed, signing bonuses are common. Often, the compensation offered must be attractive enough to draw them away from government service.

Computer forensics professionals need the right equipment to complete their work. Testing every piece of equipment and software is highly recommended to keep surprises to a minimum. The surprises occur when integration of products creates exceptions to anticipated outcomes. Equipment for the field and a lab would include imaging software, forensic tools, licenses, and hardware. Hardware includes such things as storage media, computers, adapters, and storage lockers. A basic forensic lab could easily cost $100,000 or more.

Forensic tools are best supported with assistance and training in how to use the tools. Some software packages include training and some provide training for an additional cost. There are even some organizations that only provide training in using a collection of quality forensic tools. Fees vary from being part of the purchase price to as much as $5,000 for a week of training. Most older and respected training courses are for law enforcement only.

That is changing, however, and the number of training courses offered to computer forensic professionals in corporate America is increasing. You should also consider the travel cost and loss of production incurred by the professional who attends the session. Some of the training classes can be brought to your organization if the economics are right. New technology may require yearly supplemental training for your professionals.

During certain situations, you may want to use outside resources to meet your computer forensic needs. This is often the case when dealing with unknown or unfamiliar technology. The cost of hiring an outside professional varies based on a number of factors. The three major considerations are experience of the professional, actual service, and market price. Pricing structures are based on either hourly or daily

rates. Hourly rates can vary from $100 to $500. I have heard of some daily rates being as much as $5,000. Travel expense should also be determined to get a true picture of the overall cost.

You might expect that the rates would go up for more experienced professionals, but experience alone should not be the sole factor. What services will actually be performed and what the final work product looks like are generally more important. One word of caution: there are a number of ways to complete a computer forensic engagement. Some practitioners take more time than others. Sometimes the situation dictates a particular method; however, when there is a choice, make sure that you are paying for the most cost-effective method. An example would be imaging a hard drive. If you can use the parallel port or the SCSI card to image a hard drive, the SCSI card is generally more reliable and completes the task in about half the time. (When you are paying an hourly rate, this can add up in a hurry.)

INTANGIBLES

Preferences and expectations can guide you on the intangibles of outsourcing vs. building your own computer forensics group. Performance measurements often drive these decisions. Experience is probably the common denominator of most of these measurements. Questions will arise, such as Will errors due to the inexperience of personnel be O.K.? Can lengthy time delays due to inexperience be tolerated? Where can additional information and resources for unfamiliar circumstances be found? Does the computer forensic professional have enough legal background to understand the dynamics of both criminal and civil situations?

The level of expertise provided by the professional can be very valuable in resolving issues. Headaches, dollars, and confidence are tied to how well the forensic professional can work in even the most difficult of situations. I say this because, in most situations, the meter is running. Stress has a tendency to mount when the board of directors is asking for answers. If your in-house group cannot instill confidence in your decisionmakers, its cost may not be worth it. In this situation, it is better to shop around for a resource that is a good fit for the organization.

Two recent situations demonstrate this nicely. In both, a corporate network had been compromised, and its board of directors was demanding answers about the identity and integrity of the network. In the first situation, the questions were asked and answered with confidence and accuracy by an experienced computer forensic professional. Because of the information the board received, it was able to understand the issues and feel comfortable with a "hands-off" approach given to the CIO and their staff.

The other situation was not as favorable. The IS group was confronted with a new problem. They could not generate accurate information, which led to a low level of confidence on the part of the board of directors. Needless to say, the board asked for continuous updates, and the team working on the issue spent a significant amount of time just communicating with the board — time, that might have been better spent working on the issue.

Having access to computer forensic experience leads to timely and accurate information. The first priority in these situations is getting information fast. It is only after some time has passed that questions about accuracy can be verified. Being right about both is the only thing that is acceptable. Experience is often underrated because we believe that things will turn out as planned. Experienced professionals draw upon previous situations to overcome setbacks and unplanned events. Seasoned computer forensic professionals are prepared for all possibilities when responding to an incident.

A computer forensic professional must have a good understanding of both criminal and civil law, because often the inci-

It is absolutely paramount that every case being worked by the professional be handled in a manner consistent with a criminal investigation.

dent is still of unknown origin. The victim might decide to press charges in criminal court or choose civil litigation. It is absolutely paramount that every case being worked by the professional be handled in a manner consistent with a criminal investigation. The burden of proof in a criminal court is "beyond a reasonable doubt," whereas in a civil court it is "a preponderance of the evidence." To the inexperienced person the difference might not sound like much. The difference in the eyes of the court is substantial. The issue here is that once your standard of evidence collection has depreciated to the level of proof required by a civil court, it is almost impossible to return to the standard of criminal evidence collection. It is very easy to meet the burden of proof in a civil court coming from an evidence collection standard of a criminal investigation.

Can the computer forensic professional be qualified as an "expert witness?" If yours does not have a track record of conducting computer forensic reviews, expect the opposing attorneys to beat on his credentials. The professional must withstand this test because unless he passes it, nothing else really matters. The methodologies that the computer forensic professional uses will also be tested. The training courses discussed previously use a forensic methodology that has been tested in court and a laboratory environment to confirm what is taught.

How quickly you can get information on a particular computer security event is often the difference between identifying the culprits and their actions and simply wondering what happened. With air travel today, a person can be on the opposite end of the country in four to six hours. International travel is a whole other issue with work permits, passports, and travel logistics. The point is that having a resource on the ground within 12 to 15 hours of an incident is not unreasonable. The ultimate is having a computer forensic professional on the site in a 24 x 7 capacity. The unfortunate fact is that unless you have a lot of incidents, his down time will make him feel like a Maytag repairman.

Can you find the necessary resources to complete the work within a short timeframe? Most incidents require a number of people over a short period of time, which cannot be stretched out. If a house is burning, time is limited; the resources must be concentrated over a short timeframe. I stated earlier that the value of forensics is in providing accurate and timely information to make decisions. Take the "timely" part out of the equation, and the value becomes nearly worthless. The value of the weather forecast, "It's going to rain next month" is not as valuable as "It's going to rain tomorrow." Consider this factor in your decision as well.

You now have a good basis to consider buying or renting your computer forensic capability. Large organizations that experience numerous events are often the best candidates for having an in-house computer forensic group. Medium-sized organizations with a larger number of incidents can also be good candidates for an in-house computer forensic group. A capable computer forensic partner can provide tools, training, and support for unexpected situations — consider this your Plan B. Anticipating your use of these services can also help you determine where it makes the best sense to get your resources. It is clear from trends in technology that the computer will become an even stronger part of who we are. As the computer becomes increasingly integrated in the world, we are going to need the information it provides to understand what we cannot see. Business records will be computer data. The question remains; Do you have the right kind of information?