NAID - KEEPING ITS EYE ON THE DATA DESTRUCTION BALL

How extreme focus has made the National Association for Information Destruction (NAID) so successful at what it does.

by
Bob Johnson

NAID is not your typical non-profit commercial trade association. True, like other trade associations, it is structured to serve the needs of it members, but it does so with a very specialized, deliberate and limited strategy; focusing its efforts solely on creating demand for its members information destruction services.

Its tactics are unconventional, as well. Throughout its 17 year history, NAID has operated more like a consumer advocacy organization. NAID helps reputable service providers prosper by shedding light on disreputable industry practices and allowing consumers to get the service they pay for and deserve. We also work to encourage legislation that forces organization to properly destroy discarded consumer information. At their core, both of these tactics are consumer protection initiatives.

Of course, there is an aspect of this approach that some might consider a drawback. By and large, NAID does not fulfill the role of the traditional trade association by trying to be all things to its members. For instance, NAID would not be inclined to become involved in a government relations initiative that may affect its members but has nothing to do with information destruction or information protection. Nor would NAID pretend to have any expertise in the area of environmental controls or regulations.

NAID knows data security, data protection legislation, and secure information destruction better than anyone else. By sticking to what we know, we have become the single most trusted industry authority and watchdog in the minds of service providers, the government, private sector businesses and, increasingly, in the minds of consumers.

FOCUS HAS EQUALED SUCCESS FOR NAID AND NAID CERTIFICATION

NAID is now considered a success by virtually every measure.

Membership in the organization now exceeds 1,800 member locations. It continues to add members at the rate of almost 1 per day. Much of that new membership comes from the electronic information destruction sector, as well as from international interests. Membership outside the U.S. now constitutes approximately 20 percent of member-locations, and NAID has strong active chapters in Canada, Europe, and Australasia.

NAID's certification program has also grown steadily over the last 10 years. Although the program is voluntary, almost 900 (about half) of all member-locations are now NAID AAA Certified. NAID AAA Certification is often a required vendor specification in the U.S.; present in thousands of public sector contracts, and a countless number of private

contracts. Serious information service providers openly say that NAID AAA Certification is a virtual requisite for doing business in the hard copy destruction industry.

As a testament to its level of acceptance in the marketplace, the US Department of Veterans Affairs, the largest healthcare network in the country, recently mandated that all data destruction service providers seeking their business must be NAID AAA Certified to be eligible.

Just two years ago, a full seven years after the launch of the physical destruction program, NAID created a separate certification for organizations that sanitize (overwrite) hard drives. Originally, six of the most highly regarded Asset Management companies in the country participated in the beta release of the program, with five more joining their ranks in the second year.

But devising an audit for sanitization operations posed some new challenges for NAID. Unlike physical destruction, a "wiped" hard drive looks a lot like an unwiped drive. As a result, NAID had to dig a little deeper into the processes.

To accomplish this, NAID auditors, specially trained Certified Protection Professionals (the highest ASIS International security accreditation), show up at the door of the sanitizing operation with two drives storing known content in hand. These are called the "control drives." The auditor then follows one of the control drives through the entire process, from receiving to final quality control, confirming that each step matches the company's written procedures. The second control drive is then wiped while the auditor completes the physical security and employee screening portions of the audit. Finally, the auditor pulls two random drives from the applicant's inventory, leaving the audit with the two control drives and the two random drives, all of which are then sent off to one of the most respected forensic labs for validation.

Of course, validation of the drives is only one aspect of the process. The NAID auditor will also verify quality control logs, randomly test employees' knowledge of the policies, and inspect CCTV image capture, as well as alarm logs. These steps are standard for both of NAID's Certification audits.

A LITTLE HELP FROM OUR FRIENDS

While NAID had no shortage of talented and smart people available to it from within its membership, it did not rely solely on in-house capabilities. In moving from the realm of physical destruction to that of e-destruction, NAID engaged the services of Dr. Simpson Garfinkel of Harvard University. Dr. Garfinkel had made a name for himself as the preeminent authority on sanitization when, while at Massachusetts Institute for Technology, he conducted a study that showed a significant number of second hand hard drives still contained personal information from a prior life, even though in some cases wiping had been tried. This study ended up as the seminal work on that subject titled *Remembrance of Data Passed: A Study of Disk Sanitization Practices*, (IEEE Security and Privacy – Jan '03). The take away from the study, and what NAID was seeking from

Dr. Garfinkel's involvement, was that sanitization serves as a secure reasonable method of electronic data destruction when done correctly – but that it is a process that requires diligence, appropriate operator training, and quality control systems to do it properly.

NAID also uses multiple outside advisors that serve on two of the three NAID councils that develop and protect its certification program. By definition, these outside advisors must be accredited in a discipline that compliments data security, privacy or information management. Their purpose is to represent the interests of the consumers that rely on NAID Certification and to bring a discipline-specific perspective to the program.

The NAID Certification Rules Committee, which is responsible for developing the security and audit specifications, has two outside advisors, as does the NAID Certification Review Board, which is directly responsible for dealing with non-compliance issues and other threats to the integrity of the program.

The NAID Complaint Resolution Council, which applies due process to allegations of ethical violations, does not have outside advisors in the same sense but does maintain outside legal counsel. (Yes, NAID considers non-compliance with its certification specifications, or any action that puts the program at risk, to be an ethical violation.)

A BREED APART

Both NAID Certifications, the one for physical information destruction operations and the one for sanitization operations, differ markedly from other certifications in a number of important ways.

The first difference is the cost. Ironically, while it is widely regarded as among the most detailed, rigorous and robust certification programs available, it is relatively inexpensive. NAID AAA Certification for physical destruction is less than $1,000 per year and NAID AAA Certification for sanitization operations costs about $2,500. This fee includes the price of all audits.

A more significant difference, from an efficacy standpoint, is the audit methodology itself. While NAID Certification does include a regular scheduled audit, it relies on the surprise unannounced audits as the backbone of ongoing compliance enforcement… and for good reason.

According to Holly Vandervort, NAID Certification Program Manager, "When we started the unannounced audits four years ago, we discovered that non-compliance was six times higher on the surprise audits than it was when they were scheduled ahead of time. So we doubled the frequency of the surprise audits and we instituted some fairly strong penalties. Now the non-compliance rate for unannounced audits is dramatically lower in line with that of the scheduled audits."

When Ms. Vandervort adds that "our members' clients appreciate that an unannounced audit can happen any day," she is referencing the fact that members sometimes find the

NAID auditor at their door to conduct a second or even a third unannounced audit within days of a previous audit. “Keeping everyone on their toes is critical,” cautions Ms. Vandervort.

“The lessons of the NAID’s experience have implications for all compliance certifications,” says NAID Deputy CEO Dustin McKissen. “Any program that is based solely on scheduled audits is suspect as far as we are concerned. It is easy to be compliant once a year when you know the auditor is coming. Those who ignore that fact, like we originally did, are fooling themselves, as well as the customer who relies on their certification when selecting a vendor.”

Understandably, NAID considers self-certification programs, or “auditless” certifications to be extremely misleading and harmful to customers who might be fooled into relying on them to make buying decisions. We have seen firsthand how the lack of audits and enforcement make regulations meaningless to customers. NAID has found the same thing is true on self-certification initiatives.

WHERE NEXT?

From an electronic destruction perspective, if the future does not belong to solid state devices (SSDs), they will at least be an equal partner.

NAID is already working hard to modify the current certification for sanitization operations to include the wiping of SSDs in smart phones, computers, and tablets. But, when it comes to protecting the integrity of the NAID brand, the association doesn’t take these issues lightly. There is a considerable amount of due diligence that comes first.

NAID is already engaged in research to demonstrate whether or not SSDs can be wiped and, if so, how best to do it. Some recent research has hinted that the “secure erase” function built into modern SSDs may not be completely trustworthy. NAID will find out. Other research has already made it clear that, as with sanitization of hard drives, the efficacy of the process is largely dependant on the techniques, diligence, acumen, and quality control processes of the person (or organization) doing the wiping.

The good news is that NAID has already has the right people, both inside the organization and outside the organization, to create a program that will surely enhance the association’s reputation and credibility… and, most importantly, provide consumers with program they can trust when hiring a vendor.

CUSTOMERS NEED MORE THAN A FALSE SENSE OF SECURITY

It seems like a new certification program springs up every time we turn around.

Too often certification programs succumb to the risk of making their standards and enforcement so lax that they are eventually perceived as something that can be bought-and-paid-for instead of being earned.

Too often, certification programs are tempted to be everything to everyone. They risk their hard-earned and well-deserved credibility on one issue, by speaking to an issue they know little about using criteria that is often non-specific, self-serving and meaningless.

NAID Certification will continue to focus on the one thing it knows better than anyone - Data Destruction. NAID Certification will continue to be as low cost as possible, while representing the highest level of integrity and enforcement. With that strategy, and with the ongoing recognition that strategy brings our way, NAID Certification will continue to the win the hearts and minds of consumers, regulators and elected officials who are looking for meaningful vendor qualifications amid a sea of vendor alternatives.

At NAID, we remain focused on the philosophy and strategy that earned the reputation and success we now enjoy. We will continue to stick to the principles that have served our members and their customers so well for the last 17 years.

Bob Johnson is the Chief Executive Officer of NAID. He can be reached at rjohnson@naidonline.org.