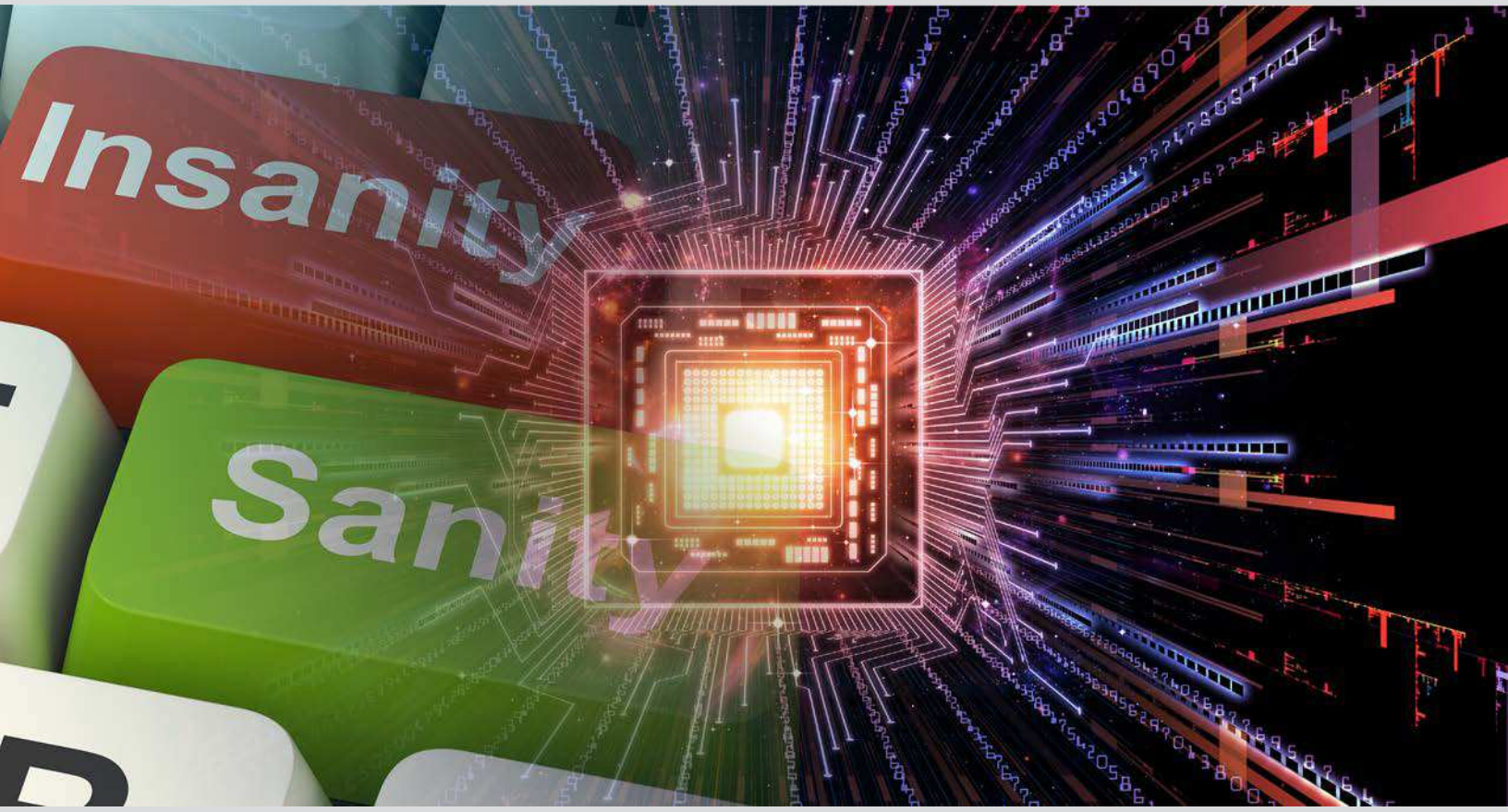
Absio®

Take Control of Your Digital World SM



Cyber Sanity

Cyber Sanity

Insanity has been defined as "doing the same thing over and over again and expecting different results." In the context of cybersecurity and online privacy, we are currently proving that maxim.

Since the dawn of network computing, we have repeatedly tried to "secure" our networks and digital data. After thirty years of failure, it's time to take a different approach to the problem.

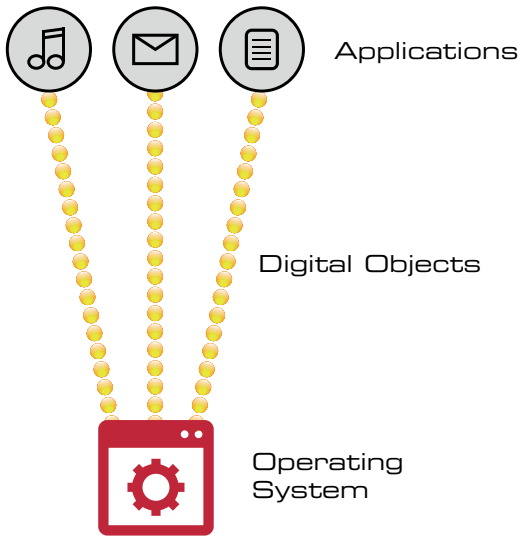
In this paper we will:

- » Demystify digital data
- » Explain the shortcomings of traditional cybersecurity
- » Present a new approach to the problem using data controls
- » Explain how to implement data controls in the real world
- » Address legal, risk management, and national security policy
- » Demonstrate the inevitability of a shift from cybersecurity alone to complete data control

Demystifying Digital Data

The digital data we create, store, and distribute using computers is physical in nature. Data can be electrons flowing through a circuit, magnetic or optical patterns on media, radio waves, or patterns of light shining through a fiber-optic cable.

Digital data is organized into digital objects. Digital objects are physical representations of bits. They have boundaries, precise formats, and information payloads. Digital objects are created by software applications, and are jointly managed by software applications and operating systems.



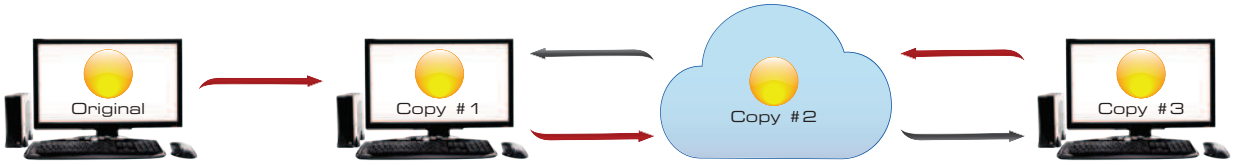
Digital objects are manufactured. They do not occur in nature. Like every other manufactured good, it is possible to engineer better ways to build, store, transport, and consume digital objects that yield increasing control and safety.

Digital objects spend most of their time accumulating in storage. The percentage of digital objects in motion at any given moment is tiny compared to the percentage of digital objects at rest in storage.

Digital objects are invisible, nearly weightless, and precisely structured. They are intentionally designed to be easily copied. Digital objects proliferate at an immense rate, because every computer attached to the internet is, in effect, a copy machine attached to a global shipping and receiving service.

In networked systems, digital objects are rarely physically moved from one device to another. Instead, digital objects are typically distributed by copying. A copy of the digital object is created and transported from Computer A to Computer B, with the original remaining on Computer A.

To compound the problem, most networked applications generate multiple copies of the digital object. First, a copy is made on Computer A. This copy is transported to Computer B. Computer B contains a shared storage space (usually a server), so that Computer C can access the digital object and copy it to Computer C. The object now exists on Computers A, B, and C. This process occurs over and over.



Why Does Cybersecurity Keep Falling Short?

Traditional cybersecurity assumes that the original method of controlling information is still broadly applicable.

In the early days of computing, control of digital information was accomplished by physical perimeter security. People could not get into the building containing the computer or carry bulky physical media out of the building without permission and witnesses. Physical perimeter security worked to control access to and the distribution of digital objects. In digital terms, perimeter security is focused on the computing environments that contain the data; it consists of controls such as firewalls, passwords, VPNs and device management.

Perimeter security started failing as soon as networks arrived and a clear physical perimeter no longer existed. However, most people still think and talk about controlling digital information in the paradigm of perimeter security. This is why we spend billions of dollars on cybersecurity with little discernible effect, and why we have little online privacy.

The purpose of networks is to share information. This is accomplished by distributing copies of digital objects, so they can be used by multiple providers to deliver information services. The common cybersecurity mantra "we need to protect our networks" is profoundly off point. Networks are not being stolen or abused, digital objects are.

We intentionally send digital objects to locations we do not own or control, so that we can get the information we need and want. Reliance upon perimeter security alone cannot successfully control digital objects that are invisible, nearly weightless, have no identifying marks, are easily copied, and travel at close to the speed of light. Rather than "secure" our data, we need to be able to *control* our data.

What is Control?

The control of digital information is the ability to determine who can access information payloads contained in digital objects, and constrain the use of the information payloads in normal and adverse conditions.

The basic level of control we want over our digital information is quite simple. We want to

determine who can access the information, constrain how they can use the information, and know what they did with the information.

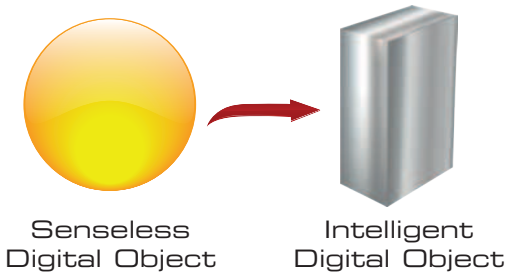
If the information payloads are highly valuable or dangerous, we can gain even more control by combining controls on the information payloads with controls on the computing environment (such as biometric authentication and device fingerprinting). We can limit which computers can be used to access particular information payloads, specify locations and timeframes for payload usage, and destroy payloads if their control is in jeopardy or lost.

The Basis of Control

Current methods for the creation, manufacture, storage, transport, and management of digital objects do not provide any significant control of information payloads. Applications automatically create digital objects without any controls or "sense". The objects do not contain rules about who can access their information payload or what can be done with information once it has been accessed. These senseless digital objects give up their information payload to any application that asks for it. They do not know where they are or where they have been, do not know who created them, and do not know who has changed them or what was changed. Senseless digital objects are inherently vulnerable to infiltrators, malicious insiders, user errors and policy/procedure workarounds. Alarmingly, the vast majority of our digital assets are stored in objects that behave senselessly, even when they are in an adverse environment.

Control begins with changing the default state of stored digital objects. Since each object has a specific format, and the format cannot be changed, the controls must be built around the object. There is no reason why senseless digital objects cannot be engineered to be intelligent by default.

The first job of control is to deny access to the information payload in the digital object. In that state, simply copying digital objects from media, or intercepting them in transmission, provides no useful information. Intelligent Digital Objects (IDOs) are undecipherable by default and can contain any data format. IDOs consist of an information payload, access permissions and usage rules, along with provenance information used to create an audit log. IDO controls persist throughout each digital object's lifecycle and work across multiple platforms, applications, operating systems, and networks.



That is a profound state change. Preventing loss of control by physical copying or interception makes the job of the hacker much more difficult. It also means that data breached from storage or by interception is provably encrypted, and is, therefore, not a reportable breach per state and federal statute.

Digital objects must have their controls momentarily removed when being processed in a computer's memory. While this creates a brief instant of vulnerability, taking momentarily senseless digital objects from memory requires the successful installation of rogue software

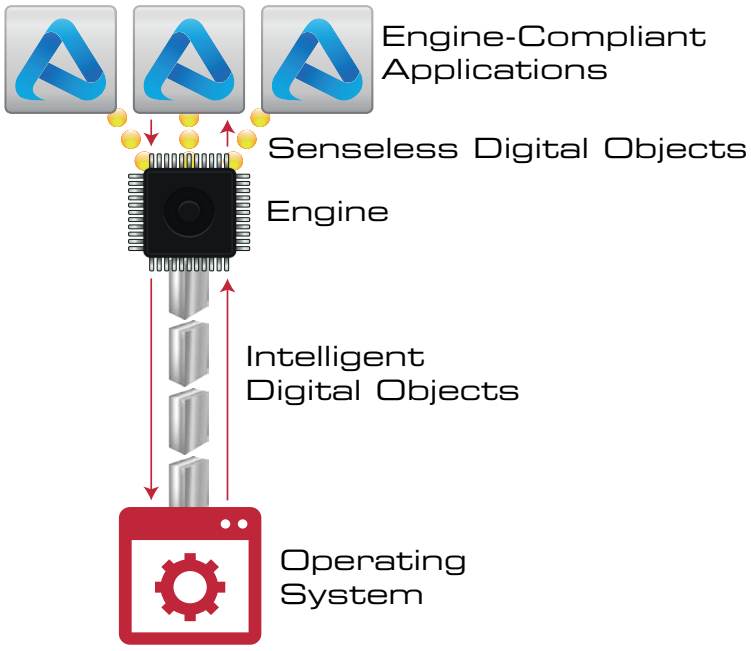
(usually referred to as malware) on a specific device, and then processing the information without getting caught. It is a difficult process and, in most cases, will provide access to a relatively small body of information, especially when compared to the volume of information that can be gleaned by simply copying senseless objects and walking out the door with them, or taking them from a lost or stolen device.

Products and processes that prevent the installation or operation of malware are rapidly gaining traction in the marketplace. Combining them with intelligent digital objects helps to thwart attacks on data in storage, in movement, and in memory. The ability to radically increase the difficulty, cost, and risk of large-scale data theft is within our reach.

Practical Implementation

There are billions of computers connected to the internet that contain trillions of senseless digital objects. So, how do we get them under control?

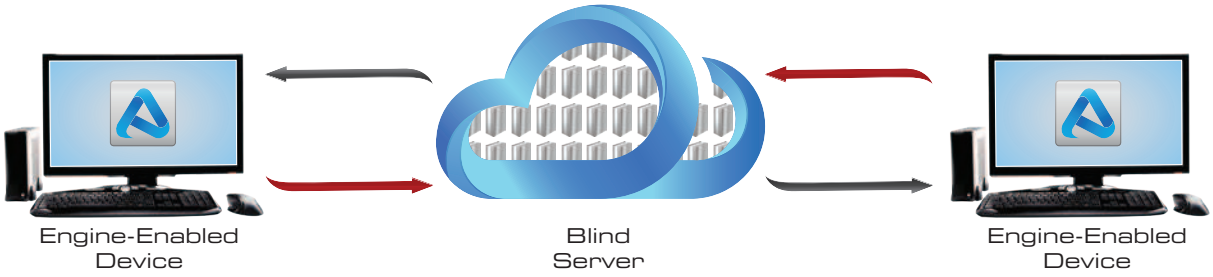
The first answer is to insert a control-creating application between the software and the operating system, so the software can create and use intelligent digital objects. Let's call that application the Intelligent Digital Object Engine, or "Engine" for short. By interposing itself between an application and the Operating System, Engine intercepts senseless objects created by the application and transforms them into intelligent objects. When Engine opens an intelligent object, it evaluates the control information and passes behavioral instructions, along with the appropriate portion of the information payload, to an Engine-compliant application.



Engine-compliant applications allow sensitive information to be securely created, processed and stored on edge devices or in the cloud. Controls are enforced even when devices are disconnected from the network or on networks the user does not control. Controls persist even when networks are compromised, devices are lost or stolen, or users don't follow policies. Applications, not people, enforce policies and procedures regarding access to and use of information.

The second major component of a comprehensive control system is a "blind" server. Practical deployment requires services such as transport, remote storage and backup, user directories, application stores, audit, and application validation. Blind servers deny service providers any ability to remove controls from users' digital objects. Blind servers cannot be the source of a reportable breach.

The combination of Engine and blind servers, in conjunction with good perimeter security, can form the first truly effective and comprehensive data-control architecture.



To encourage wide and rapid deployment, Engine needs to support any type of data, be installable on multiple operating systems, be efficient enough to run on computers ranging from smartphones to servers, and simplify the control problem for developers.

Engine will require improvements to current applications, which will take a significant amount of work. However, software is constantly being updated and improved, especially when the improvements are driven by marketplace demand. Software and information service providers that deliver persistent control and privacy to their customers gain a huge advantage in comparison to providers that do not.

Policy

Current policymakers view cybersecurity and privacy violations as the result of some form of breach. Policy does not currently address the fundamental question: why should a breach yield any intelligible data? Policy that reinforces the paradigm of perimeter security alone will only produce continued failure.

Legislators and regulators are preparing to create prescriptive rules for industry that will not solve the actual problem. They are expected to tell industry how to solve the cybersecurity and privacy issues, rather than setting a performance standard and encouraging industry to develop the solutions. The NIST Cybersecurity Framework standards, which contain many useful practices, are in jeopardy of being turned into compliance regimes that cannot solve the problem. Prescriptive regulation will enable the software and information services industries, with the willing cooperation of regulators, to be absolved from liability even while harmful losses of data continue to escalate.

As an alternative approach, we can look at what has worked in other industries. When there was a rash of disasters in petrochemical plants around the world in the late 1980s and early 1990s, the initial regulatory response was an attempt to prescribe how plant operators should build and operate plants. However, the industry worked out a much better approach with OSHA. OSHA gave plant operators five years to develop, implement and document their safety plans, and required the industry to provide that documentation to OSHA in the event of a problem. That information is also available to the tort bar. The industry became religious about safety, rapidly innovated, and got much better at keeping hazardous chemicals under control. Perhaps even more importantly, the insurance industry worked closely with the petrochemical industry to

develop metrics and control standards that made understanding and managing risk a contributor to profit rather than a sink for costs.

The legislation and regulation of the software and information services industries should be handled in a similar fashion. As a policy matter, senseless digital information should be seen as safety issue, because it makes using computers and computer-controlled infrastructure potentially unsafe. We now know that senseless data can be highly hazardous to individuals, organizations and national security. The software and services industries will build and use intelligent digital objects when it increases profits and avoids liability.

Inevitability

Every day, organizations grow more worried about maintaining the confidentiality of their digital information, and individuals grow more concerned about maintaining their online privacy. Cybersecurity spending is up — way up. To date, attempts to control digital information have proven to be complex and tedious, because we have not put available, but unused, processing power to work to make the job more simple.

Over the years, Microsoft's MS-DOS® gave way to graphical user interfaces. Software that used to require specialized expertise to operate gave way to applications that almost anyone can use. Finding, ordering, and shipping a product across the country used to be a major undertaking – now it is trivial. Desktops shrank to laptops and then to smartphones and tablets. It used to take elaborate planning to get work done on the move; now it is a matter of course. All that simplification is a result of intelligently harnessed processing power and good software engineering.

The three elements required to make the shift from senseless digital objects to intelligent digital objects are in place: abundant processing power, software engineering know-how, and market demand. The shift is inevitable.

When people can easily exercise whatever degree of control they want over their digital information, what requires significant effort today will quickly become ubiquitous, and will ultimately be demanded. Smart software and service providers will learn that they can increase revenue, market share, and profit by cooperating with their customers' desire for control. The computer industry has never let resources go to waste for long, and it will not do so this time either. Control creates far too many opportunities.

We have witnessed three great waves of change in the digital world since the mid-1980s. First came personal computing. Then came the commercialization of the Internet in the mid-1990s, giving us connected computing. Then roughly ten years ago, mobile computing exploded on the scene. The next great wave, just now beginning, is controlled computing — we will be able to keep all of the gains of the last 30 years — but now, we can reclaim our freedom — our privacy, through personal control.

Absio Corporation
8740 Lucent Boulevard, Suite 101
Highlands Ranch, CO 80129

Sales/Support: 720.836.1222

www.absio.com

110-WP002-2