Rethinking Cybersecurity
“It is not about the networks, it is about the data. It is the data that is valuable, and it is the data that is risky.”

GUS HUNT, FORMER CHIEF TECHNICAL OFFICER, CENTRAL INTELLIGENCE AGENCY (2012)

THE FAILED FORTRESS

The conventional approach to cybersecurity is failing because it focuses on the wrong things. Anyone who reads about cybersecurity has heard the endlessly repeated platitude, “We need to protect our networks.” Are networks really what we are trying to protect? Stuck in a fortress mindset, we focus on perimeter security, strengthening the walls and posting more sentries, assuming that a perimeter exists that we can defend and that housing our data inside the perimeter will give us control.

Imagine for a moment that we replaced currency with pieces of paper anyone could copy. How much sense would it make to build stronger bank vaults and post more guards if everyone could make as many copies of those pieces of paper as they wanted? Would it make sense to move those pieces of paper around in armored cars, or to store them in vaults at work and at home? For every piece of paper held in a vault, how many copies would the holder not know about? Would it make any difference if you kept bad people outside the vaults or armored cars? Would it make any difference if you could tell that bad people had gotten inside and carried out some of those pieces of paper? Would any set of walls, guards and procedures accomplish control, or would they just create a local illusion of control?

A one hundred dollar bill is an analog object that carries an information payload, and has multiple controls built into its structure—controls intrinsic to the object. The micro printing, holographic ribbon, mag strip, serial number, paper and ink are intrinsic controls in the substance of the bill itself. Intrinsic controls focus on use. They assure that the bill, regardless of person, time, place or circumstance of use, delivers its information payload (i.e. this represents $100 of trade value to you and anybody else you give it to).

Vaults, guards, and alarm systems are extrinsic security. Extrinsic security is outward facing; it divides the world into outsiders who are not trusted and insiders who are. Extrinsic security is about constraining access. Intrinsic controls are about assuring reliable and predictable use. No array of extrinsic security measures can protect objects that lack intrinsic controls, especially objects that have to be distributed to be useful.
Cybersecurity has always focused on extrinsic security. However, the product of computers and networks is data. Therefore, the value and the risk of network computing are in the data. How does cybersecurity change if you want to control the data itself?

**FIRST PRINCIPLES**

Thinking about cybersecurity from the standpoint of the data can be difficult. It’s easy to get lost in the details and complexity of the fortress model. To take a fresh look at cybersecurity, let’s review first principles of data and software.

**What is digital data?** Data that is carried in digital objects. Digital objects are structured and encoded bundles of zeroes and ones (files) that contain information payloads. Data is broadly defined. It includes everything that conveys meaning: messages, documents, outputs from databases, images, video, audio, paid content, etc.

**What produces and manages data?** Software. Software is comprised of digital objects that contain instruction payloads. The instructions operate the computer and manage the data.

**How are digital objects distributed?** Digital objects are distributed by making copies. We rarely actually move digital objects (deleting the original after copying), so copies proliferate wildly. Much, if not most, of your data is copied to computers you don’t control and, unless you are the developer, software always comes from computers you don’t control.

**What are the states of digital objects, and how many are in each state?** Digital objects can be at rest (in storage), in motion (in transit from one computer to another), or in use (loaded from storage into memory). The vast majority of digital objects are at rest. Tiny percentages are in motion or in use at any given time.

**In what ways can digital objects be encoded?** Digital objects can be encoded in cleartext so that the information can be freely read, or encrypted so that the digital objects cannot be read unless specific conditions are met. Encrypted objects are also referred to as ciphertext.

**In what ways does encryption protect digital objects?** Encryption can be used to make objects unreadable, prevent unknown changes, sign objects to make them unique and identifiable, help identify legitimate users of objects, and prevent eavesdropping on connections between computers.

**What governs the application of encryption?** Compute power (operations per second). Today, there is sufficient distributed compute power to apply encryption to all data, at rest and in motion, everywhere,
all the time—provided that software is engineered to take advantage of the compute power. The abundance of compute power can also be used to assure the integrity and provenance of software.

Does encryption apply to all data? No. Currently, data in use (loaded into memory and being processed) cannot be encrypted.

CHALLENGING CONVENTIONAL WISDOM
Rethinking cybersecurity with intrinsic control in mind turns conventional wisdom upside down. The following are a few examples.

Investing solely in more elaborate extrinsic security is a waste of time and money. Typically, over 30 different extrinsic cybersecurity solutions are deployed in a large enterprise. They are complex to configure and require constant attention from people that are hard to find. Requiring more cybersecurity tools than you can afford and more people than you can hire is the relentless reality of the last 15 years. There is no indicator that more spending on extrinsic security will produce better results.

Previous investments in extrinsic security measures were in no way a mistake. They were all that could be done with available compute power, but that constraint is gone. Extrinsic security that obscures pathways to systems and data, thwarts malware, gathers and disseminates threat intelligence, and prevents denial of service attacks are all still necessary. It will require the combination of extrinsic security and intrinsic controls to be highly effective.

People are not a big part of the solution. People are not able, no matter how well trained or motivated, to reliably implement or manage policies on data distribution and use. The volume and diversity of digital objects is too great, decision-making is too complex, and too much of the data is out of our reach. Control will come almost exclusively from software engineering. People cannot reliably enforce data distribution and use policies, but software can.

Protect all data equally, not just data that is “important.” First, we are rarely certain what data is important. Some is important because it is obviously valuable, like trade secrets or paid content. Some data with no obvious value is important because it could cause trouble if it got into the wrong hands. Some data is not important in isolation, but is important when aggregated. If we limit the data we protect, we inevitably fail to protect some that is important.
Second, protecting part of the data makes that data an obvious target for attack.

Third, using multiple systems to provide disparate controls on different bodies of data is more expensive than using a common method for protecting all data.

Fourth, even if we are successful in identifying data that merits protection, we rarely ever know where all the copies of the data exist. For example, people who feel protected by their secure document repositories rarely take into account the dozens of copies in unsecure email or copies held by outsiders.

Finally, requiring people to continually make and implement decisions about the importance of data forces them to choose between security and getting their jobs done. They often develop workarounds when security procedures disrupt their normal workflow. To be effective, you have to protect all data with intrinsic controls from the moment of creation.

**Focus on high-bandwidth vulnerabilities, not low-bandwidth vulnerabilities.**

High-bandwidth vulnerabilities enable attackers to take a lot of data per exploit. Low-bandwidth vulnerabilities typically garner relatively little data per exploit. Cybersecurity tends to focus on low-bandwidth vulnerabilities and ignore high-bandwidth vulnerabilities. Below are two examples (there are many others):

— Cybersecurity has paid far more attention to outsiders than insiders. Industry and practitioners prefer not to talk about the insider threat; there is no viable solution for it. The aim of almost every exploit that starts on the outside is to masquerade as a legitimate inside user or software application. The high-bandwidth vulnerability is “legitimate” inside users.

— Transmission security (encrypted connections between computers) is the definition of cybersecurity in the minds of many, but the focus on transmission security has obscured the high-bandwidth vulnerability—data stored as cleartext. If data is stored in encrypted objects, the data is protected when those objects are copied and transmitted, regardless of the type of connection.

**Limit reliance on perimeter security to data in use.**

Because processors cannot handle encrypted data in memory, perimeter security that keeps exploits, technical and human, away from data in memory is essential. The two mistakes we keep on making are: 1) assuming extrinsic security applies to data in distribution, and 2) failing to apply intrinsic controls to data we do not intend to distribute, such as internal data stored in large-scale financial and healthcare processing systems.
VULNERABILITIES
Below are the primary vulnerabilities for data listed from higher bandwidth to lower bandwidth. Bear in mind that this analysis applies to your data on your devices, your data on other people’s devices, and other people’s data on your devices.

Data stored as cleartext. This is by far the greatest vulnerability. It is the jackpot for attackers; they need only bypass the perimeter. It makes the insider threat impossible to mitigate effectively, and weakens every other possible control.

Weak authentication. Not knowing with certainty who is using the computers that contain your data is the next major vulnerability. Simple username and password authentication is woefully insufficient.

Malware. Malware typically does one or more of the following: bypasses weak authentication to capture credentials, invades legitimate software, copies stored data, captures data from memory, prevents your access to your data, or uses your device to stage attacks on other people’s devices.

Uncontrolled redistribution. People in your organization, doing their jobs correctly, send your data to users and computers outside your control. Your data can be redistributed from other people’s computers without your consent or knowledge, by other people or by malware.

SOLUTIONS
Solving the problem requires a change in focus from extrinsic security to intrinsic control—from focusing on networks to focusing on software. Software applications that provide intrinsic control for data are control-enabling applications. Control-enabling applications meet these criteria:

— Applications must build cryptographic controls into the objects they generate. This enables control to persist no matter who acquires the objects or how they acquire them.

— Applications must store and transmit intrinsically-controlled objects. At a minimum, every object must be encrypted and accessible only by users with cryptographically-validated credentials.

— Applications must embed controls in each individual object (granular control). Single controls that span too many objects create unwanted exceptions to control and prevent specificity of control. For example, whole disk encryption only provides control when the system is not in use. When a user logs in, whole disk encryption no longer provides control. Preventing a particular email from being forwarded, or preventing the alteration of a particular document, requires controls specific to the individual email or document.
Applications must be able to use strong authentication and apply that authentication to specific digital objects. This means that strong authentication is required to open a particular file or to run a particular application.

Applications must verifiably honor controls embedded in the objects. Data control is irrelevant if the software used to access the digital objects does not provably persist the controls.

In addition to control-enabling applications and strong user authentication, accomplishing intrinsic control requires:

- **Control over software installation.** Encrypting stored objects does not reduce this requirement; it will only shift the focus from malware that exfiltrates cleartext data to malware that attacks applications and memory. Rigorously evaluate anti-malware; most products do not deal effectively with the volume of and rapid change in exploits.

- **Assurance from third-party providers.** IT service providers and software vendors must provide assurance regarding what they do with your data. Do they store your data in cleartext? Can they work with your controlled digital objects? Do they provide clear contractual assurances about how they handle your data? Select third-party service providers and software vendors that support your controls.

**ASK THE RIGHT QUESTIONS**

Unlike fortress cybersecurity, intrinsic control provides a path to success. Goals and progress are measurable, more resources are available, and people are not required to do the impossible. Implementing intrinsic control of your data is a significant departure from traditional cybersecurity. Developing the rationale for making that change requires that senior business and technical management address the right questions. Below are some questions to consider.

**Is our data valuable enough to make it worth controlling?** If it is, then start working on intrinsic control.

**Is there enough risk in our data to make it worth controlling?** If we cannot control our data, is our reputation at risk? Or our customer’s confidence? Or our business partnerships? Are we at risk of violating regulations and being fined or sued?

**How can we prevent our systems from being used to invade other people’s systems?** At a minimum, your organization should consider controlling software installations and using strong authentication to prevent the use of your organization’s systems to attack others.
Can our investment in intrinsic control generate a return? Like network and mobile computing before it, intrinsic control is a fundamentally disruptive technology. Can you distribute your data without diminishing its value? Can you increase trust in your organization? Can you improve the value of your software offerings? Can you offer a new approach or a different business model? What opportunities are there in providing control in an out-of-control world?

These questions are not about compliance. Current compliance standards do not address intrinsic control. If, after analysis, you are willing to assert that your data has little value or risk, other people’s data stored in your systems also has little value or risk, and there is no other opportunity for return, do not work on intrinsic control. Compliance is sufficient.

RUINING THE ECONOMICS OF HACKING

The term “hacking” once meant breaking into systems. It now describes taking data by any means and for any motive. Employees about to leave their job hack their employers for data they can take to their next job. Outsiders, ranging from professional data thieves to nation states, hack companies to take trade secrets or other valuable information, to embarrass the organization, or to stage a larger attack. Paid content is hacked and redistributed without attribution or payment.

A hacker’s ability to profit is based on a specific technical condition: when hackers get your digital objects, they have your data. When a hack yields your digital objects, but those objects yield no data, the hack is a failure. Intrinsic controls ruin the economics of hacking.

ABOUT ABSIO

Absio provides a new approach to information security—the ability to secure and control your data everywhere, all the time. Current cybersecurity technologies focus on indirectly controlling the environments that house data in storage and in transit, but do not control the data itself. Absio’s patented technology builds controls into each unstructured data object, where any use or exchange of the data is at the owner’s discretion. Originally developed to encrypt and control intelligence data in a battlefield environment, Absio now offers its technology commercially to organizations looking to secure their data by default and control it on demand. Absio Dispatch® is an easy-to-use, multi-platform email application that automatically secures and controls messages and attachments everywhere they exist, with enterprise administration and archiving capabilities.