FORTRA™

5 Myths Holding Your Security Program Back

By Dr. Dan Geer

Introduction

Thanks for picking up this Quick Guide. Maybe you head information security at your organization. Maybe you help set your company's data governance policy. Maybe you work with partners and suppliers and worry about protecting the wider data supply chain. In any case, you are seeking insight into how your data protection regime can be more efficient and effective.

As cybersecurity professionals, we share the somewhat unfortunate job of trying to protect our network and data assets from cyber-attack. One can rightly argue that cybersecurity is the most intellectually demanding profession on the planet. The rate of change is so great that no challenge is ever solved, no problem ever resolved completely. That said; security failures more often result from a lack of direction and focus, not of a lack of skills or resources. The press loves to report our failures – so this increased scrutiny requires of security professionals our best effort.

Security industry legend Dan Geer argues that there are five misconceptions common to many data protection programs that are in actuality retarding these efforts. These five "myths" were selected because they address pain points common to many organizations … maybe even yours. Successfully addressing them will give you and your ongoing protection regime reasonable assurance of some quick wins.

In reviewing this list, continue to ask yourself how to apply the advice to your organization and your unique cybersecurity ecosystem. The myths endeavor to challenge you a bit on how you think about the difficulties we all face.

Myth 1 - Security success depends on the level of control you have over your environment.

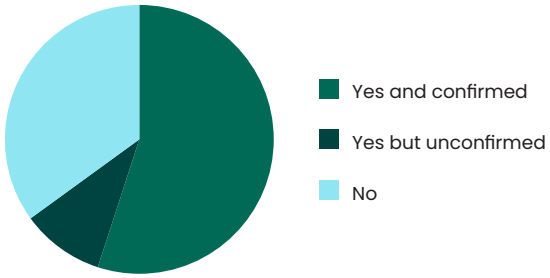
The Reality

Ultimate success in cybersecurity will never result simply from implementing more stringent controls. What's more important is having better visibility of your organization's data.

Data is where the true value is. Our opponents are after the ability to see it, to affect it, to gain an advantage by possessing it. This fact is as common to large scale attacks on government and military targets as it is to breaches suffered by small businesses. The success measures of every cyber-attacker are: What did we get? Did we get it without being noticed? Can we use what we got for monetary gain or strategic advantage?

Just having controls everywhere is insufficient. If your controls fail, chances are you won't even notice. If someone steals your car, you notice. If someone steals your data, you still have it. Data can be stolen without you even knowing it. Most data breaches are discovered by a third party, not the victimized organization.

The Index of Cybersecurity, a monthly measure of CISO confidence, asked respondents if they had ever discovered someone else's data loss, where the victim was unaware that a breach had occurred.



The Verizon Data Breach Incident Report found 80% of data losses are discovered by a third party, not by the victim.

Myth 1 - Security success depends on the level of control you have over your environment.

The Answer

Don't be a control freak. Focus on creating better data visibility, not better controls. Controls cannot be effective without real visibility of data movement. Cyber criminals may not grab our data on first access; they may just come in and look around. You can sometimes catch them in reconnaissance, but not always.

Therefore the greatest point of risk is when your sensitive information is on the move – when data at rest becomes data in motion. This transfer of data across time or location should be the primary focal point of any successful security regime.

With better visibility into what is happening with your data, the controls you develop will be more intelligent.

"The greatest point of risk is when your sensitive information is on the move – when data at rest becomes data in motion."

Myth 2 - Effective data protection must start with a lengthy and complex data discovery and classification process.

The Reality

Data discovery and classification are highly important, but also need to be practical. To avoid being victimized, you must undertake some effort to complete them. Still, it's disabling to your efforts to march step-by-step in a linear quest to attain the perfect schema. There is no perfection in the business of cybersecurity. Here is one example where "the best" is definitely the enemy of the "good enough."

Continue to measure the success of your discovery and classification procedures to make mid-course corrections, but get to your data protection schema as soon as possible. Discovery and classification should be an ongoing process that's never complete.

"Data classification is important, but be practical. There is no perfection in the business of cybersecurity. It's disabling to your efforts to march step-by-step in a quest for linear perfection. The best is the enemy of the 'good enough.' Get to the data protection scheme asap."

Myth 2 - Effective data protection must start with a lengthy and complex data discovery and classification process.

The Answer

Start by building a baseline set of protections based on data context instead. There are fewer kinds of context than there are types of data. Start with the assumption that breaches are inevitable. Base your contextual hierarchy on where your most critical intellectual property resides. If yours is an engineering firm, then the most important IP is its designs and drawings. If you are a stock exchange, then it's trading floor data. It might be lab test results for a pharmaceutical organization, and so on.

Context requires thinking about probable breach scenarios. Start with the assumption that someone will always get in. Focus instead on blocking or blunting the effect of an attacker's potentially malicious activities. Ask "If someone got access, what would they do?" There are most likely a small and reasonable number of potential actions. Focus on these versus protecting all data access points.

Combining this newfound contextual awareness with data transfer visibility makes your data protection schema more scalable. Data volume is only growing, so this requires thinking about scale early and often. Consider the way anti-virus vendors think about malware: there are too many varieties to count, there's more propagating every day, and new strains are mutating constantly. The same can be said for cyber-attack methods.

"Start with the assumption that breaches are inevitable."

Myth 3 – The goal of cybersecurity is to keep the bad guys out.

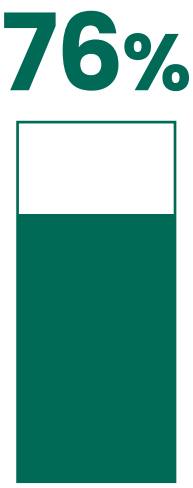
The Reality

Twenty years ago, this is what the information security profession tried to do. Today it's impossible. Simply put, some of our adversaries are too skilled to keep out. In the national security world, this is called "intrusion tolerance."

In our increasingly interconnected world, what do "in" and "out" even mean anymore? Retailer Target was breached via its HVAC contracting firm. Were they to be considered inside or outside the company?

The first measure of success of any external attacker is to gain the credentials, authority and access rights of an insider. Anyone who steals these should be considered "inside." Anyone who has access is potentially a threat, including employees engaging in risky behavior, unintentionally or otherwise. Watching network traffic is important, but keeping your network clean simply isn't good enough any longer.

Outside threats look like insiders:



76% of network intrusions exploited weak or stolen credentials.

Myth 3 - The goal of cybersecurity is to keep the bad guys out.

The Answer

Today, the goal of cybersecurity is not to keep the bad guys out, but rather to keep the valuable data in. Focus on data movement, not what type of attacker is trying to obtain it. Protecting data in context means limiting or preventing what adversaries can do once they are in.

What we today call the “insider threat” is in reality the true threat. Designing data protection regimes around insiders by default also protects against any outsider posing as an insider. The outsider attack problem is solved as a side effect – with ruthless efficiency.

What are your employees allowed to do and not do?

The goal of this inside-out approach is to keep sensitive data from getting out. Egress filtering becomes more important than ingress filtering. Sure, screen for malicious email, but don’t allow any data movement in outbound network traffic to go unnoticed.

"The goal of this inside-out approach is to keep sensitive data from getting out."

Myth 4 – Data surveillance means breaking employee trust and invading employee privacy.

The Reality

Surveillance has become a loaded word. There's a lot of it these days. We are all surveilled whether we like it or not – for example, each and every one of our smartphones is tracked by geolocation.

The proper level of acceptable surveillance is a matter of debate inside each individual organization. As cybersecurity professionals, we must ask these questions: What is fair to do? What is not fair to do? What can be done safely (vs. unsafely) to protect the organization's critical IP?

But surveillance need not be an attack on employee privacy rights. It's not about the organization reading every email. Reading every email may identify single security incidents, but it won't reveal the more powerful insight: patterns of data movement and their context.

"We read everything" is a policy never well received. A better approach for implementing data surveillance is the one common to European businesses that are subject to Workers' Council regulations. These regulations require anonymization of employee information and obfuscation of file contents in surveillance efforts. These constraints are well considered, if not always well implemented. North American businesses may choose to rely on this model.

It is important to reassure worried or angry employees that your surveillance efforts will focus on total scrutiny of data movement, not data content. This focus on data in context will address the privacy concerns of most worried parties, if correctly presented.

"We read everything" is a policy never well received. A better approach for implementing data surveillance is the one common to European businesses that are subject to Workers' Council regulations."

Myth 4 – Data surveillance means breaking employee trust and invading employee privacy.

The Answer

Context is more powerful than content. What's of paramount importance is that data is moving and how. Rights and permissions are easier to set and enforce than deducing user intent. Similar to security clearance regimes in a classified setting, you may ask, "Does the user in question have a 'need to know' the information they are attempting to transfer?" Still, establishing data flow patterns will be more powerful than tracking any single incident.

Event data for all forms of data movement can be collected without examining actual file contents. It can be anonymized yet still descriptive of the types of users, files, repositories and applications involved. Defining responses based on context will help prioritize your surveillance efforts.

"Defining responses based on context will help prioritize your surveillance efforts."

Myth 5 – If you can secure your own environment, your data is safe.

The Reality

Yes and No.

As the Target incident proved, any third party who can see your data is a potential risk, even if they don't have full access rights. An organization's data supply chain is populated by both secondary and tertiary data sources, typically third party vendors and suppliers. Chances are that Lockheed Martin stores fighter jet plans for the Pentagon.

Today's hackers are increasingly sophisticated and resourceful, no longer "living in their parents' basements." Any determined attacker knows how to work the data hierarchy progressively from tertiary targets up to secondary and ultimately primary targets.

"Any third party who can see your data is a potential risk, even if they don't have full access rights."

Myth 5 - If you can secure your own environment, your data is safe.

The Answer

If the Homeland Security Administration is thinking about the data supply chain, you should too. A complex data supply chain calls for a collaborative approach between partners, suppliers and other stakeholders. One could argue that Home Depot should have better coordinated data protection with its point-of-sale terminal vendor.

Reach out to your peers at these organizations. Use a common language when discussing your data. Discuss their ability to help protect your data when they access it. Try to run the same technology – that's a consistent control. This includes managing use of public cloud services and following the same guidelines set by applicable regulatory authorities. If you can, mandate that third parties adopt your security practices up and down the data supply chain.

Summary

If you meet someone who's been working in cybersecurity for a long time, the first question you should ask them is why haven't they solved it? The simple reality is that the discipline of cybersecurity has become so complex that no one can keep up with every aspect of its strategy and application. As Donald Rumsfeld so eloquently put it, "There are 'unknown unknowns.' We don't know what we don't know." Cybersecurity expertise requires all of us to become specialists.

Security regimes age, while both data volume and data valuation are only rising. Cybersecurity expert Bruce Schneier believes "complexity is the enemy of security". Simplify by focusing, not on individuals or networks, but on the data. Strive for greater visibility of data in motion. Focus on data context, not user intent. Make discovery and classification an ongoing process and automate that process based on context. Build a security strategy focused on keeping valuable data safe. Implement data surveillance, but make it known to employees that their privacy will be protected. Collaborate with partners to secure your data supply chain.

Pursuing data-centric security puts you in a better position to weather the withering rate of change in our industry.

"Complexity is the enemy of security."

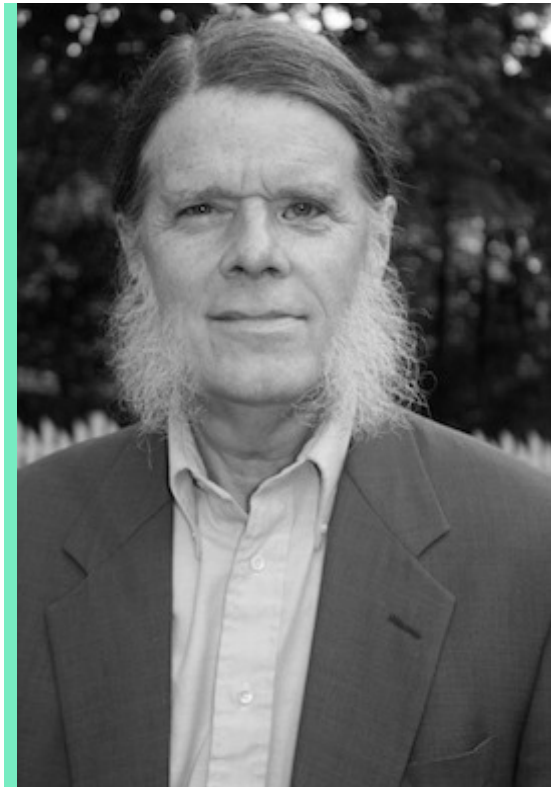
- Bruce Schneier

About Dr. Dan Geer

Dr. Dan Geer is currently the CISO for In-Q-Tel, a not-for-profit investment firm that works to invest in technology that supports the missions of the Central Intelligence Agency and the broader U.S. intelligence community.

His history within the security industry is both extensive and striking. Looking at just a few of his accomplishments, Geer was a key contributor to the development of the X Window System as well as the Kerberos authentication protocol while a member of the Athena Project at MIT in the 1980s. Shortly after, Geer created the first information security consulting firm on Wall Street in 1992, followed by organizing one of the first academic conferences on electronic commerce in 1995.

Geer is also the past president of the USENIX Association where he earned a Lifetime Achievement Award. Often cited for his thoughtful security philosophy and deep industry expertise, Geer has testified before Congress five times and has consulted with numerous startups and their investors.



About Digital Guardian

At Digital Guardian, we believe in data protection. We know that within your data are your company's most valuable assets. The sum total of innovations, plans and potential. We protect your company's sensitive information like it's our own so you can minimize risk without diminishing returns.

For over 10 years we've enabled data-rich organizations to prevent data loss at the endpoint. Our expert security team and proven Digital Guardian platform radically improve your defense against insider and outsider threats.

Hundreds of customers across a wide range of industries rely on Digital Guardian to protect their critical information at the point of risk. Seven of the top ten IP holders and five of the top ten auto companies trust us with the integrity of their most valuable and vulnerable data. We take pride in knowing that, at this very moment, Digital Guardian agents are securing the sensitive data of the world's most inventive, influential companies.

More information at **www.digitalguardian.com**.

Special Offer

Are you interested in taking the first step to data-centric security?

The Digital Guardian (DG) Visibility Study is a great place to start. It will provide you with actionable intelligence on policy compliance, privileged user and insider activity, and potential targeted cyber-attacks.

You install the DG endpoint agent on 50 or more endpoints (maximum 150 endpoints) and we take it from there. The program will run for 90-days, but after just 30-days we'll provide you a detailed snapshot into how your sensitive data is being used, or in some cases, misused.

The DG Visibility Study Program is completely deployed and managed by Digital Guardian data protection experts and our agent continuously monitors the activity of your sensitive data against insider and cyber threats both on and off your network. It requires no staffing or hardware from you.

The Visibility Study requires NO customer resources:

- No hardware
- No licensing
- No security expertise
- No staffing

Just email us at **info@digitalguardian.com** and we'll have a DG Account Manager explain how to get started.

WE'RE FOCUSED ON PROTECTING ONE THING

DATA

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-dg-gd-0423-r1-79d