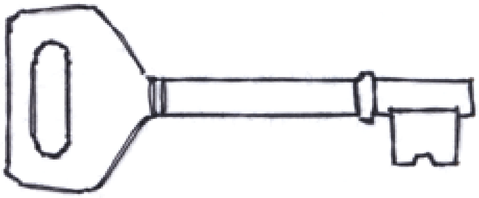

[MYTHS] AND [FACTS] ABOUT DATA SECURITY

Companies need to tell their data stories, but misconceptions are holding them back, say Brunswick's GEORGE LITTLE and SIOBHAN GORMAN

Cybersecurity is a pressing and poorly understood issue across all sectors. With big names such as Target, JP Morgan Chase, Sony Pictures Entertainment and health insurance giant Anthem in the digital crosshairs, CEOs and boards are zeroing in on cybersecurity threats as a growing risk to their businesses.

While security is the central concern, it is increasingly important that companies get ahead of the communications curve to develop and defend not just data, but their own narrative. A company's data story should explain to both the public and employees how the company is benefiting from the collection and analysis of data – a critical issue for many investors – and how they are acting responsibly to protect it.

Unfortunately, misunderstandings about data security and hacking are hampering efforts to develop and communicate effective strategies. With anxiety high as a result of headlines and public outcry around high-profile breaches, these false impressions are keeping corporations on the defensive. Here are some myths that have emerged around corporate data security – and why they're wrong.

[MYTH]

YOUR COMPUTER NETWORK IS SAFE IF YOU HAVE A STRONG ENOUGH SECURITY "FENCE"

[FACT]

There is a "new normal." Every fence has holes. Hackers will find a way into your system, so you need to plan for that eventuality by enhancing the internal protection of your most critical data. You should also think ahead about how you will explain a hacking episode publicly. What story do you want to be able to tell when – not if – your company has a breach?

[MYTH]

ALL SECURITY INCIDENTS ARE CREATED EQUAL

[FACT]

Hackers have different methods and objectives when accessing corporate systems. Like robbers rattling doorknobs to find an unlocked house, hackers test security systems all the time. Some merely probe networks, while others seek to steal, manipulate or destroy data. The information they target varies with the intent, from customer credit card data that they can steal to sensitive internal communications, research and development projects, or full customer profiles that can be used to expose or embarrass the parties involved.

[MYTH]

THE GOVERNMENT WILL HELP WITH A BREACH

[FACT]

You're mostly on your own. In many countries, companies learn they had a security incident from a government agency, but often the assistance ends there. For major events where officials are interested in information about how a hack was executed, the government might offer investigative or forensic help from law enforcement and intelligence officials. But governments are sometimes wary – for legal or political reasons – of helping companies fix their computer systems or of retaliating against the believed perpetrator of a hack on behalf of a company or group of companies. Governments have their hands full protecting their own networks.

[MYTH]

BREACH INVESTIGATIONS WILL QUICKLY TELL YOU WHAT HAPPENED

[FACT]

Companies usually discover breaches long after they occur, and forensic investigations often take weeks or months to produce data. Even when complete, those investigations sometimes can't pinpoint who was responsible for the hack. It's important to manage expectations within a company during an investigation about how much information will likely be gleaned about the hack.

[MYTH]

COMPUTER SYSTEMS SECURITY IS JUST AN INFORMATION TECHNOLOGY PROBLEM

[FACT]

People, not software, tend to be the weakest link in data protection. A study by computer security firm Trend Micro found that 91 percent of cyberinfiltrations began with “phishing,” where malicious links are embedded in emails sent to unsuspecting employees or customers. Recipients unknowingly grant the hacker access to their computers when they click on the link.

[MYTH]

COMMUNICATING ABOUT A CORPORATE BREACH MUST BE REACTIVE

[FACT]

Plotting out a communications strategy in advance for different types of data security problems will help a company understand the risks and plan for them. It’s also worth thinking about what data the company has that could be damaging to it – or others – if released.

[MYTH]

ALL HACKING IS A CYBERATTACK

[FACT]

There are many flavors of hacking, and the most common types are not attacks but network infiltrations to steal corporate secrets. Cyberattacks that manipulate or destroy data or computer systems are still relatively rare. However, these attacks have been on the rise, as seen recently with the breach at Sony Pictures that both destroyed data and exposed embarrassing company communications.

[MYTH]

BREACHES MUST FIRST BE HANDLED BY TECHNICAL AND LEGAL EXPERTS AND ONLY LATER SHARED WITH OTHER KEY PEOPLE IN A COMPANY

[FACT]

Given the reputational risk a breach generates, an organization’s communications team should be involved in early discussions about the event to provide guidance on how to ensure the company maintains the trust of the public. The team should also be well versed in cybersecurity basics before a hacking incident, so it can quickly get up to speed when one occurs.

[MYTH]

WITH A BREACH, THE BIGGEST PROBLEMS ARE SECURITY AND LEGAL ISSUES

[FACT]

The greatest threat a breach poses is ultimately to corporate reputation. While the need to fix security problems and address legal issues is clear, companies may not realize that how they discuss the event publicly at the outset will often determine whether they can recover the confidence of the public – and investors – once it is over. Companies that change their story over time risk a more severe loss of that trust.

GEORGE LITTLE is a Partner in Brunswick’s Washington, DC office. A former Pentagon Press Secretary and chief CIA spokesman, he advises on cybersecurity, privacy and data security, and crisis communications.
SIOBHAN GORMAN is a Director in Brunswick’s Washington, DC office. Formerly a reporter for *The Wall Street Journal* on national security, she advises on public affairs and crisis handling with a focus on privacy and data.