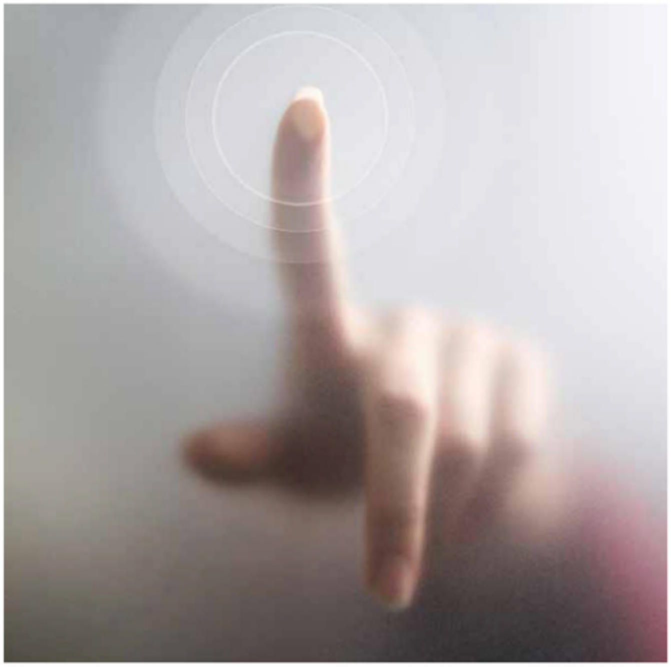
At the Edge of the Cloud

THE FOG



Having become accustomed to all the implications of governing information in the cloud, information governance professionals are well-positioned to lead their organizations into "fog computing," ensuring that they are taking advantage of its benefits while mitigating its risks.

Brent Gatewood, CRM

With information governance (IG) professionals having achieved a relative level of comfort around governing information in the cloud, now their world is becoming "foggy."

Fog computing, according to Cisco's Maher Abdelshkour, is "a new model to ease wireless data transfer to distributed devices in the Internet of Things (IoT) network." In a company blog (*http://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing*), Abdelshkour provides Cisco's lengthy definition of fog computing, stressing how it stretches cloud services to improve the user experience:

> [Fog computing is a] paradigm that extends Cloud computing and services to the edge of the network. Similar to Cloud, Fog provides data, compute, storage, and application services to end-users. The distinguishing Fog characteristics are its proximity to end-users, its dense geographical distribution, and its support for mobility. Services are hosted at the network edge or even end devices such as set-top-boxes or access points. By doing so, Fog reduces service latency, and improves QoS [quality of service], resulting in superior user-experience.

Describing the same thing, IBM calls it "edge computing." In an IBM blog at *https://www.ibm.com/blogs/cloud-computing/2016/01/cloud-computing-move-to-the-edge-in-2016/*, Andy Thurai explains it as a drive to move "from the central cloud platforms toward the edge, or toward decentralizing the cloud. This is partly because, with the proliferation of IoTs, operations technologies (OT) and decision intelligence need to be closer to the field than to the central platform."

Why Fog Computing?

The driving factors for moving to fog computing are escalating data volumes and the lagging Internet bandwidth.

Escalating Data Volumes

Computer users are creating content at an incredible rate. According to IDC's "The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East – United States," the United States will be creating 6.6 zettabytes of information per year by 2020. This growth is compounding at a rate of more than 25% annually, meaning this number doubles in three years' time.

By 2020, it's also estimated, more than 35% of that information will be touched by the cloud. In the United States, then, 2.6 zettabytes of information will be processed, managed, or moved by the cloud. This volume seems like just the thing for which the cloud was designed. And it was – but there is a complicating factor.

Lagging Bandwidth Growth

In the computing realm, Moore's Law states the number of transistors on a circuit board will double every two years. Intel's David House relates Moore's Law to the processing power of computers doubling every 18 months. So, there should easily be computational capacity to create 6.6 zettabytes of information annually by 2020.

However, the growth of Internet bandwidth is not close to keeping pace with Moore's Law. In 2014, it was actually closer to 50% (rather than 100%) every 18 months, according to Michael Enescu, then the chief technology officer of Open Source Initiatives. And, a 2013 study by TeleGeography that compares the growth rates of regions across the globe shows the United States and Canada are trailing other regions in bandwidth growth. (See *www.telegeography.com/products/commsupdate/articles/2013/10/31/africas-international-bandwidth-growth-to-lead-the-world/*.)

This means the ability to access, process, and transmit data is not keeping up with the volume of data being created. This will ultimately lead to congestion, affect system reliability, and make it difficult to prioritize data. Data loss will rise, Internet response times (latency) will increase, and the usefulness of data will decrease.

The easiest ways to minimize the consequences of rapid, escalating data growth and lagging bandwidth growth are to: 1) reduce the amount of data being transmitted and 2) move the data and computing centers closer together. The movement of data to the "edge" of the cloud and devices to the edge of networks enables fog computing.

Devices on the edge of the network will need to do more to get the right data in the "big data" mix. Not only will they need to create, collect, store, and act on information as it is gathered, they will have to decide on the types of information that must be saved and transmitted to other systems. This means that some information will not be managed by cloud or on-premises controls. Thus, IG must be extended to the fog also.

Where Is the Fog?

Information is collected and processed by IoT-connected devices around the world and throughout all industries, so the fog is descending on every organization. An ever-growing number of processes and tools is managed by smart devices and appliances, which gather, process, and transmit immense amounts of data.

For example, equipment in manufacturing facilities constantly monitors itself for maintenance and supply purposes and shares this diagnostic data about the machine and its environment with the organization using the machine, the machine's vendor, and the parts supplier.

Not just the line of business tools and applications are gathering information. So are the tools used to manage facilities and make working lives easier or more convenient.

Right now the footprint of these tools may be small, or the deployment of IoT may be insignificant within some organizations, but it is growing and will continue to grow. It is expedient to address the fog's unique requirements now, while the exposure is minor.

What Are the Fog's Risks?

Organizations that are collecting and transmitting data that never resides in a controlled repository and is not managed by their own IG rules, are at risk.

For example, in the previous scenario, a machine on the manufacturing floor may be gathering and sending information to a vendor about supplies the machine needs. Among the data being gathered, though, there may be information about machine calibration or preventative maintenance that has been performed that the organization is likely required to manage for a defined period in a defined manner.

If this information lives in the fog on the edge of the organization's systems, it may never be managed in conformance with the organization's rules. It may be maintained for a period that is inconsistent with those rules, and it may even be shared with vendors when it should not be.

Organizations that are not aware of their devices in the fog and the rules that govern them are at risk. And, even when organizations are aware, security and privacy risks are great if governance measures have not been applied or if they have been applied haphazardly through a combination of rules that were arranged by the system vendor, its implementer, and the system owner.

To mitigate these risks, organizations must be aware of which systems are collecting, processing, storing, and transmitting information. They must know what information is being collected and shared and with whom it is shared. They must vet these processes against the organization's IG policies or procedures, and they must ensure that these policies and procedures relate to IoT systems and devices.

What Are the Next Steps?

The fog represents significant opportunities for organizations. They will find – just as they did after experimenting with cloud computing – using applications and appliances on the edge, in the fog, will work or is already working for them. By providing an enhanced ability to collect and react to information quickly, fog computing gives its users a competitive advantage today. But tomorrow it may be a necessity for organizations that want to keep pace with competitors.

This puts IG professionals in a very good position, if they are prepared to take it.

Reach out to Management

Research this topic as it relates to the organization's industry and bring these issues to management; it is likely that no one else has done this yet. Be prepared to discuss fog computing on multiple levels. Plan to give summaries in three-minute, 15-minute, and 60-minute sessions, knowing that the audience will have little or no understanding of the technologies being discussed.

The summaries should explain why the organization should embrace IoT and fog computing and describe the IG risks associated so management understands the complete environment.

Reach out to IT

Next, speak to colleagues in IT. Assess their awareness of the opportunities and risks associated with IoT and fog computing. Ask them if:

- They are aware of any current implementations that utilize fog computing
- There were any safeguards or controls put in place to limit risk and exposure
- There is a plan in place to curate the information captured and managed in the fog
- There is an ownership model in place for fog computing and the resulting data sets

Give IG Responsibility

Add fog governance to the responsibilities of the IG committee. Awareness at that level is critical to organizational acceptance because this group has the best visibility into the organization's lines of business and the potential use of fog computing and edge-related appliances.

Additionally, this group will have the exposure to the tools used internally for administrative purposes, for it is likely that fog computing will find its way into the administrative side of the organization as well.

Develop Governance Rules

There must be rules to manage this content. Start with a policy on the appropriate use of fog computing and then develop procedures to identify and control information sets. From here, review the policies and procedures for other technologies and repositories to ensure there are no contradictions. If there are any snags, correct them.

Why Be Afraid?

The use of fog computing need not be scary to IG professionals or to their organizations; it is just another tool that needs to be understood, supervised, and maintained. IG professionals are just the right people for ensuring that!

About the Author: Brent Gatewood, CRM, is owner of consult-IG, an IG and RIM consulting firm. He has worked in many capacities in many industries to help organizations better manage their information assets. He advises clients on the use and importance of enterprise information. Gatewood can be contacted at *bgatewood@consultig.com*.