encryption of data. Distinguishing which applications are appropriate to apply encryption to from those where it is not is the crux of this first step. Essentially, the goal is to identify and record -- in as granular detail as possible -- where data an enterprise might want to encrypt resides in the cloud. For some situations (i.e., SaaS), "as granular as it gets" might be that the data is held at a certain CSP. For others (i.e., IaaS), it could be that you get down to the level of a certain virtual device or storage container. The point is, your organization should know which applications and environments process the data you care about, versus those which do not, and you should be able to construct a rough idea of where you'd need to apply controls.

If this sounds like a tall order, it can be. Start with a manageable subset and build on it. There are tools that assist in this regard. In a private cloud context or one where your business has a fairly extensive relationship with an IaaS provider, virtualization-aware tools can assist in the inventorying of specific hypervisors to help determine what's running where. SaaS discovery tools exist as well, but in a pinch some service-level information can be gleaned from examining user traffic .To automate the task of keeping track of specific systems and applications, can provide an assist as well to record services and usage as they're identified. The point is, organizations need to establish which data is in which environments so that they can prioritize their efforts.

- **Evaluating specific usage**-After data classification and service inventorying, the next step is where the "rubber meets the road." It's here where your organization must evaluate the specific usage, make the determination about whether it will encrypt, and decide how it will implement encryption. Note that depending on the cloud computing model or service your organization is using, it may need to select different tools to affect this. For example, if you have a high-sensitivity SaaS application and you want to encrypt data within it, affecting this is very different from encrypting a database within a PaaS or encrypting volume storage in an IaaS.

With an IaaS use case, for example, since you have access to the underlying OS on virtual images within that environment, you might choose to implement a tool that operates at the file-system level. In fact, Microsoft and most Linux distributions natively support encrypted file systems that may be viable options. There are dozens of commercial products that support this as well. For a PaaS, your choices might be more limited; you may need support from the developers actively working in the PaaS to author code that leverages CSP APIs or that leverage specific APIs in the application environment they're working in. And, of course, in a SaaS context, since the entirety of the application stack is managed by the CSP, you may find yourself looking to reverse-proxying tools or a specific SaaS-integrated product to accomplish that.

The point is the tools vary and these differences should be noted and planned around; if your organization needs to purchase multiple tools to do this, it will need to plan its budget accordingly. Using the inventory and data classification evaluation that you've already done can help prioritize which approach is most valuable and/or urgent.

6. Conclusion

In light of these data traffic security problems, it's no wonder that network security improvements rank among the enterprises' IT project priorities for 2015, according to the survey findings. More than half indicated that network security improvements are planned for 2015 and nearly a quarter named network security as a top IT priority for the enterprise in the coming year. In total, two-thirds of enterprises report that they are budgeting such projects. If enterprises are studying and learning from the recent parade of data breaches, then we can safely predict that several initiatives will be included in these network security projects:

1. Proactive security: More enterprises will establish proactive security and stronger network segmentation by encrypting sensitive data traffic over all networks.
2. Encryption consolidation: Reducing the number of forms of encryption and consolidating encryption control will make protecting traffic simpler and reduce the possibilities of gaps in the end-to-end data path.
3. Simpler policy management: Because all networks are essentially untrusted today, it makes less and less sense to focus solely on network-based VPNs that connect a device to a network. Instead, encryption policies are now focusing on connecting an authorized user to the applications they want to access and then applying the required encryption profile. The policy should be applied regardless of which devices or networks are involved, which in turn enables more consistent, enforceable and auditable encryption policies.

In the end, the IT security community already has benefited greatly from the lessons learned by the surge in hack attacks. IT security now has the attention of senior management and budget decision-makers. In the long run, this heightened prioritization and investment can only improve the overall effectiveness of security controls and allow them to evolve to meet the changing needs of users and applications in the modern enterprise.

References

[1] **"Cloud Computing Security Issues and Challenges";** International Journal of Computer Networks (IJCN), Volume (3): Issue (5): 2011; Kuyoro S. O., Ibikunle F. & Awodele O.
[2] "**Observing the Clouds : A Survey and taxonomy of Cloud Monitoring**"; Ward and Barker *Journal of Cloud Computing: Advances, Systems and Applications* (2014) 3:24
[3] "**Addressing cloud computing security issues**";Dimitrios Zissis ∗, Dimitrios Lekkas; Future Generation Computer Systems 28 (2012) 583–592
[4] www.techgig.com
[5] www.techtarget.com
[6] "**Exploring Cloud Computing for Naïve**";Reema Ajmera & Rudra Gautam; IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.12, December 2014 62
[7] NIST cloud definition, version 15 http://csrc.nist.gov/groups/SNS/cloudcomputing/.

Author Profile

Surabhi Shukla holds a B.E. in Computer Science, from RGPV and is currently pursuing M.E. in Computer Science at the same university RGPV. She has been involved with Infosysworld, as a business analyst for 1 year. Her interest area is Cloud Computing and database security. She is trying harder to secure database in cloud.