ARMA INTERNATIONAL Edmonton Chapter

armaedmonton.org

June 2018
Volume 1, Issue 1

Vote for Director of Membership and Bylaws

In order to move forward with the incoming board, and utilize ratified bylaws, we are required to have 50% + 1 votes from our strong membership.

We are pleased to announce that we need your vote for the Director of Membership! We have two very talented and capable members:

Kristan Cook is the Director of Corporate Information Governance for the City of Edmonton, She has a Masters Degree in Archival Studies from UBC and is a frequent speaker at Information Management conferences and events, She believes her leadership skills and experience will contribute to the continued success of the Chapter Office. Kristan thinks there needs to be a focus on increasing meaningful membership and offering value for membership. Kristan would like to create a space for collaboration and successful integration that both supports and promotes its membership through education, training, and networking.

Jordan Uytterhagan has 15 years of IT experience; 7 of which focus in ECM and Records Management, In 2015, he held office as the Director of Membership for ARMA Edmonton. The areas that Jordan feels should be focused on the most fresh, relevant programming to industry trends; involving remote members that aren't able to travel to Edmonton or take part in events. His vision for the Chapter is generating engagement and participation to contribute to creating an active Edmonton Chapter.

Bylaw Ratification
The board require your vote to approve to adopt and implement the bylaws that were amended in 2015, What has changed:

- Alignment with the standard ARMA International format, shortened descriptions of sections, changes to membership level descriptions. Please see the bylaw revisions attached to the Newsletter distribution email.

VOTE HERE FOR ALL BY JUNE 12: **https://bit.ly/2IW9744**

Save the Date!

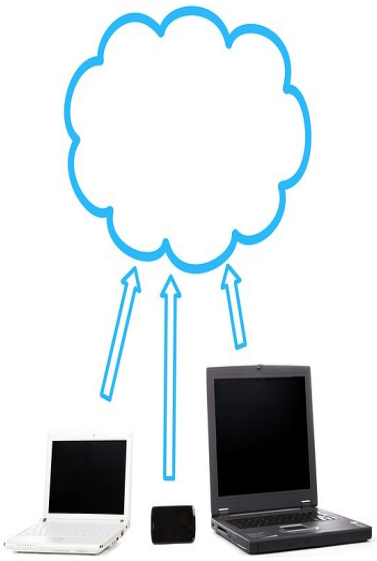
The Annual General Meeting (AGM) of the members of ARMA is coming up, and you're all invited! This free event will be held on June 13th at the CRAFT Beer Market (10013 101A Ave NW, Edmonton). Doors will open at 5:00 p.m., and the AGM will start at 5:15 p.m..

The AGM is a great opportunity to meet our new board members, generate ideas, and network with peers and other information professionals.

Light hot appetizers will be provided. However, if you have any dietary requirements, make sure to inform us by email at vicepresident@armaedmonton.org before June 6, 2018.

For more information, including the meeting agenda, check out our event page on EventBrite. Attendance to the AGM is FREE for all ARMA Members in good standing. The link is below to RSVP:

https://www.eventbrite.ca/e/arma-edmonton-annual-general-meeting-tickets-46233625017



Inside this issue

Did you know?

SaaS means "software-as-a-service". It is a "software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet"[1]. This is one of the "main three categories of cloud computing, alongside infrastructure as a service (IaaS) and platform as a service (PaaS)". [1]

1 https://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service Accessed on 3 May 2018.

Fake Requests for Payments

By Angela Watt, CIP Presdent-Elect, ARMA Edmonton

ARMA Edmonton has been receiving fake requests for payments. It is important that we validate all requests with double authorization. Please note that any communications from ARMA Edmonton will be sent with from an [at] armaedmonton.org account, and all payables will be sent through our treasurer with validation from the executive. If you have received any communications you believe to be phishing or scam, please notify us at vicepresident@armaedmonton.org.

Information Security in the Cloud

Gina Guidi, Information Management (IM) Professional

Today, businesses seeking technology solutions are presented with software-as-a-service (SaaS) options. However, storing the business's data in the cloud still causes concern. Now, the cloud isn't really a cloud at all, and the information always resides in servers...somewhere. The cloud just means that the data can be accessed through the Internet and that the business doesn't have to manage and maintain the infrastructure that the data is stored in.

But, wait a minute! Doesn't that mean the data is more vulnerable to cyber attacks?

Well, no.

Your business is probably relatively small, right? Let's say there are less than 1000 employees, but maybe you have more. Whether you're a large organization with a mature IT department or a small organization with one IT guy that needs to know it all, it's likely that your specialty is not providing data-hosting services. This means that your business doesn't have the rigorous security controls and robust safeguards that data-hosting providers do.

Below are the four major security controls and safeguards that organizations need to look for when considering cloud solutions:

1. Physical Security, which includes infrastructure location(s) and access controls, onsite security staffing and monitoring (video surveillance and alarms), and environmental safeguards, such as redundancy procedures and backup power
2. Firewalls and Intrusion Detection
3. Internal Data Access Processes
4. Information Security in the Cloud

The SaaS provider should a detailed description on each of the above controls and safeguards that they employ with any proposal submission.

How I Learned to Stop Worrying and Secure My Digital Assets in the Cloud

Peter Allen, SVP, General Manager, Data Management at Iron Mountain

Fears that data stored in the cloud can't be secured are overblown. The reality is most cloud services are as secure as on-premises data centers, provided you employ these tactics to protect against the inadvertent disclosure of customer data.

Ensure encryption. It's the single most effective protection available because if attackers gain access to your data, it's useless. Always use encryption, including while data is in transit to the cloud. Never store encryption keys in the cloud.

Use strong authentication. Believe it or not, about 80% of security breaches can be traced to compromised passwords. Passwords should be a minimum of nine random characters or strings of random words. Where possible, use two-factor authentication, which uses a second form of access control, like codes delivered by text message.

Leverage a managed service. These services save time and provide peace of mind by monitoring cloud assets to detect hard-to-catch problems like misconfigurations or insider attacks.

Know where your data is. Keeping your data at a single location can be risky so use geo-resiliency to guarantee availability. Some cloud providers move data around the world for efficiency, but that may create legal or regulatory problems. Be sure your provider observes geographic restrictions.

If you would like to contribute to the newsletter, please contact the newsletter editor:

Marlena Muskens
muskensm@mymacewan.ca