



REN-ISAC

Research and Education Networking Information Sharing and Analysis Center

REN-ISAC Mission

The mission of the REN-ISAC is to aid and promote cyber security protection and response within the higher education and research (R&E) communities, through the exchange of sensitive actionable information within a private trust community, the provision of direct security services, and serving as the R&E trusted partner within the formal ISAC community.

The following slide illustrates activities that a typical security office undertakes, and the relative benefit to those activities that the security communities REN-ISAC, EDUCAUSE & Internet2 Security Task Force, Regional and State Organizations, InfraGard, and FIRST provide.

By nature, the benefits of regional and state organizations will vary. In this representation we've attempted to hit a middle ground.

Things a security office/team does:			Regional & State Orgs		
outreach awareness and training		✓	✓		
policy development and enforcement		✓	✓		
situational awareness	✓			✓	✓
monitor for threat and infected systems	✓				
protect systems and users from active threat	✓			✓	✓
vulnerability scanning	TBA				
incident response	✓		✓		✓
data and privacy protection		✓	✓		
internal security reviews and consulting					
risk assessment		✓			
report to management			✓		
interface with law enforcement	✓			✓	
continuing education of staff	✓	✓			
evaluate security products and services			✓		
compliance monitoring		✓			

Information Sharing

- REN-ISAC is a private trust community for sharing **sensitive** information.
- The private and trusted character of the membership
 - provides a safe zone for the sharing of organizational incident experience – information which otherwise would not be shared,
 - protects information about our methods and sources, and
 - protects information which if publicly disclosed would abet our adversaries.

REN-ISAC is a Cooperative Effort

- Member participation is a cornerstone of REN-ISAC
- Dedicated resource contributors: IU, LSU, Internet2
- Advisory Groups
 - **Executive Advisory Group:** IU, LSU, Bard College, Reed College, U Mass, UMBC, Internet2, and EDUCAUSE
 - **Technical Advisory Group:** Cornell, IU, MOREnet, Team Cymru, UC Berkeley, U Mass, U Minn, U Oregon, and WPI
- Analysis Teams
 - **Microsoft Analysis Team:** IU, NYU, U Washington
- Committees
 - **Membership Committee:** Illinois, IU, LSU, Scranton, UMN, UNI
- Service development teams - numerous contributors
- Other major contributions (systems, tools, coordination, etc.)
 - Buffalo, WPI, MOREnet, and EDUCAUSE

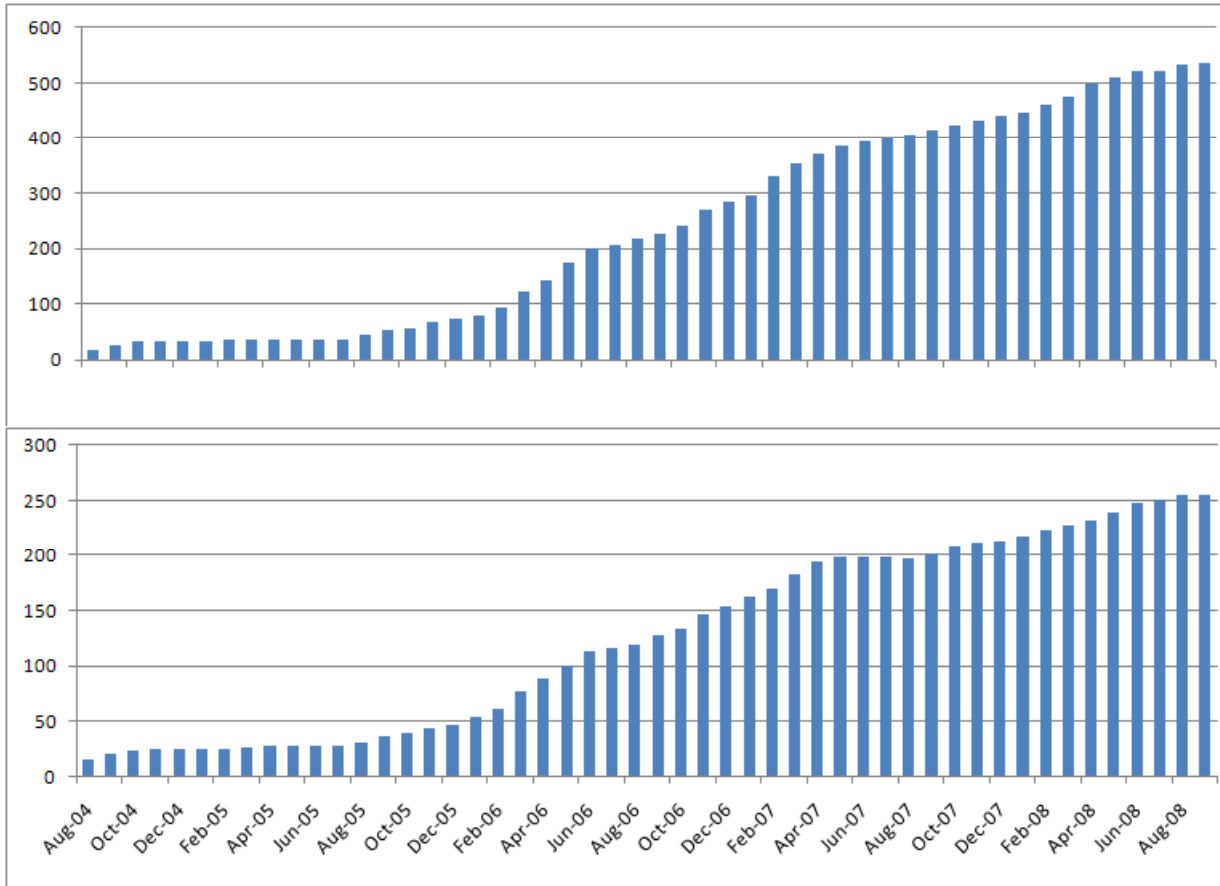
Benefits of Membership

- Receive and share practical defense information in a private trust community
- Establish relationships with known and trusted peers
- Have access to direct security services
- Benefit from information sharing relationships in the broad security community
- Benefit from vendor relationships, such as the REN-ISAC and Microsoft Security Cooperation Program relationship
- Participate in technical educational security webinars
- Participate in REN-ISAC meetings, workshops, & training
- Have access to the 24x7 REN-ISAC Watch Desk
- Have access to threat information resources ("data feeds") that can be used for IP address and DNS block lists, sensor signatures, identification of local compromised machines, etc.

Information Products

- Daily Watch Report provides situational awareness.
- Alerts provide critical and timely information concerning new or increasing threat.
- Notifications identify specific sources and targets of active threat or incident involving R&E. Sent directly to contacts at involved sites.
- Feeds provide collective information regarding known sources of threat; useful for IP and DNS block lists, sensor signatures, etc.
- Advisories inform regarding specific practices or approaches that can improve security posture.
- TechBurst webcasts provide instruction on technical topics relevant to security protection and response.
- Monitoring views provide summary views from sensor systems, useful for situational awareness.

REN-ISAC Membership



People

Orgs

A Revised Membership Model

- In Feb 2009 a revised membership model will be implemented.
- Old model: Individuals joined to “represent [the] institution”. The individual was required to meet a certain work profile and receive trustworthiness vouches from existing members.
- New model: Institutions and organizations join. A CIO or designee joins on behalf of the institution. That person assumes the role of "management representative", and nominates one or more "member representatives" who participate in the operational information sharing. Two tiers of participation are differentiated in the degree of vetting of the prospective member representative and the classification of sensitive information shared in the tier.
- Objectives of the new model are to:
 - Retain a strongly trusted information sharing environment
 - Extend the reach of REN-ISAC more broadly in the R&E community
 - Align “membership” directly with the institution
 - Set a base for a long-term sustainable business model

Membership

- Membership is open to:
 - institutions of higher education,
 - teaching hospitals,
 - research and education network providers, and
 - government-funded research organizations;
 - international, although focused on U.S.
- An institution must have a **management representative**, and one or more **member representatives**.
- Two classes of member representative: **General** and **XSec** differ in criteria for membership and in the types of information sharing and services the member representative may participate.
- An institution can have any combination of General and XSec representation.

General and XSec

- General member representatives:
 - The CIO (or Head of IT) nominates representatives – one or more full-time staff who meet eligibility requirements
- XSec member representatives:
 - To qualify for XSec, a General member representative must:
 - Have six weeks experience as a REN-ISAC General member representative
 - Be a principal security representative for the institution
 - Devote more than 50% of time to security work
 - Receive trustworthiness vouches from other XSec members
 - Submit an application
- All REN-ISAC members, as of Feb 1, 2009, have grandfathered XSec eligibility.

General and XSec

Benefit	General	XSec
Receive and share practical defense information in a private trust community	sensitive	extra sensitive
Establish relationships with known and trusted peers	yes	yes
Have access to direct security services	some	yes
Benefit from information sharing relationships in the broad security community	yes	yes
Benefit from vendor relationships, such as the REN-ISAC and Microsoft Security Cooperation Program relationship	yes	yes
Participate in technical educational security webinars	yes	yes
Participate in REN-ISAC meetings, workshops, & training	yes	yes
Have access to the 24x7 REN-ISAC Watch Desk	yes	yes
Have access to threat information resources ("data feeds") that can be used for IP address and DNS block lists, sensor signatures, identification of local compromised machines, etc.	limited	yes

Membership Fees

- The fee is per-institution, irrespective of the number of member representatives from the institution
- If one or more representatives at an institution are XSec, the institution pays the XSec fee
- Our business plan called for fees of \$900/700 XSec/General for the fiscal year beginning July 1, 2009, but due to the economic downturn, a decision has been made to scale back plans for fiscal 2009-10, and reduce fees by 50%.
- Accordingly, fees for fiscal 2009-10 are:
 - \$450/year for institutions with one or more XSec member representatives
 - \$350/year for General member-only institutions
- Fees will be re-evaluated each year.

How to Join

- Institutional membership is applied for by the CIO, local equivalent, or a designee of the same.
 - Requiring CIO or eq. involvement gives us a tractable point of reference for confirming identity, and identifies institutional commitment
- That individual becomes the management representative, and nominates one or more member representatives.
- The process will come online in February 2009.
- <http://www.ren-isac.net/docs/membership.html>

REN-ISAC Business Model

- Financial goal - Through a combination of tangible sponsorship, support, other philanthropic revenue, and fees, generate funding for sustainable REN-ISAC operations, supporting reach to all of U.S. higher education.
- All revenue generated by the REN-ISAC is used to fund services provided to the R&E community.
- Voluntary member contributions of staff time and expertise are used to keep fees as low possible.
- Financial principles and guidelines are published at <http://www.ren-isac.net/docs/charter.html>
- A financial review will be conducted once yearly with participation of the Executive Advisory Group.

Priorities for the Coming Year

- Implement the two-tiered membership model
- Implement a sustainability & growth business plan
- Membership growth
- Facilitate member involvement and contribution
- Develop additional information sharing relationships
- Assess current services and member needs
- Development projects
 - Scanning Service
 - Sensor projects (commercial and non-commercial partners)
 - Security Event System (SES), in cooperation with Internet2 and DoJ
 - Incident Information Sharing System (RENOIR), in cooperation with Internet2 and Worcester Polytechnic Institute

Other REN-ISAC Services

- REN-ISAC will continue to work with the community to identify and develop new services and information products.
- Software developed by the REN-ISAC will generally be available as Open Source.
- Over time, the REN-ISAC may add services targeted directly for individual campuses, such as log analysis, penetration testing, and network scanning. These institution-specific services may require a separate fee.

References

- REN-ISAC Organizational Documents
 - Charter
 - <http://www.ren-isac.net/docs/charter.html>
 - Membership Document
 - <http://www.ren-isac.net/docs/membership.html>
 - Membership Terms and Conditions
 - http://www.ren-isac.net/docs/terms_and_conditions.html
 - Fees
 - <http://www.ren-isac.net/docs/fees.html>
 - Information Sharing Policy
 - http://www.ren-isac.net/docs/information_sharing_policy.html
 - Disclaimer
 - <http://www.ren-isac.net/docs/disclaimer.html>
- Overviews
 - Flier
 - http://www.ren-isac.net/docs/ren-isac_brief.pdf
 - Presentation (this document)
 - http://www.ren-isac.net/docs/ren-isac_executive_overview.pdf

Contacts

Mark Bruhn, Executive Director, mbruhn@iu.edu

Doug Pearson, Technical Director, dodpears@ren-isac.net

Gabriel Iovino, Principal Security Engineer, giovino@ren-isac.net

<http://www.ren-isac.net>

24x7 Watch Desk:

soc@ren-isac.net

+1 (317) 278-6630