
ماژول 1

# اصول امنیت

C|SCU
Certified Secure Computer User

Certified Secure Computer User

# Honors & Awards

- MCSA2003-MCSA2003Security
- MCSE2003-MCSE2003Security
- Windows Server 2008 Network Infrastructure Configuration
- Windows Server 2008 Application Infrastructure Configuration
- Windows Server 2008 Active Directory Configuration
- MCITP Server Administrator
- MCITP Enterprise Administrator
- Microsoft Certified Information Technology Professional
- Installing and Configuring Windows Server 2012
- Administering Windows Server 2012
- Configuring Advanced Windows Server 2012 Services
- Microsoft Certified Solutions Associate 2008, 2012
- Microsoft Certified Solutions Expert 2012 - Server Infrastructure
- IT professional - Cyber Security Org – SANS – Cloud Security Org – Network Security Org
- Comptia A+ - Comptia Network + - Comptia Security + - Comptia Master Level Security ( CASP )
- Mcp V1, 2- MCTS
- Microsoft Certified Solutions Expert 2012 - Cloud & Security
- Microsoft Certified Solutions Expert 2012 – MSG

**Best Regards,**

**Alireza Ghahrood**

**Pm: Security Products Manager**

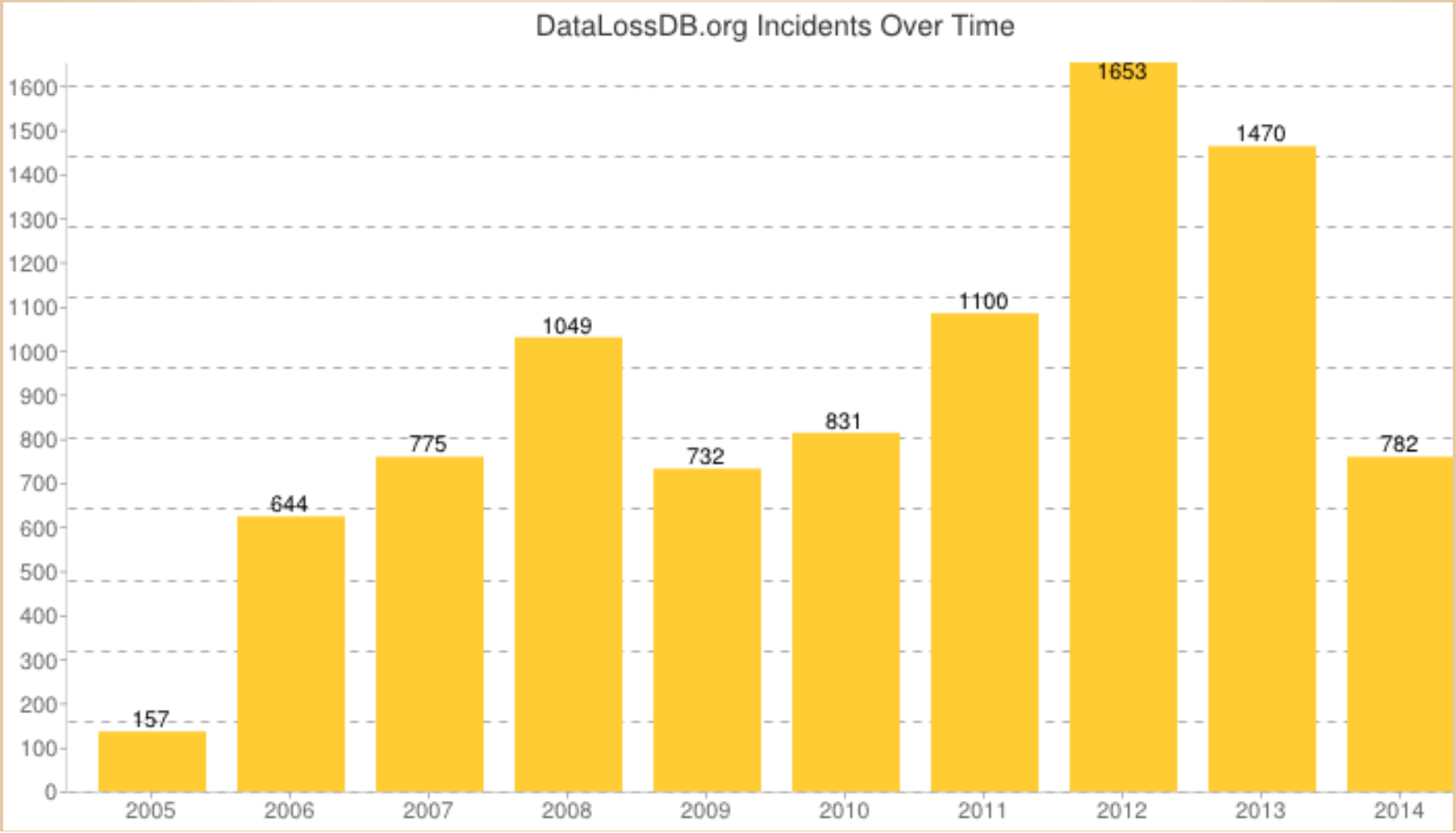
**( Security Solution Provider : Cyber Space |BigData |Cloud |Virtualization**

**Sarv Co**

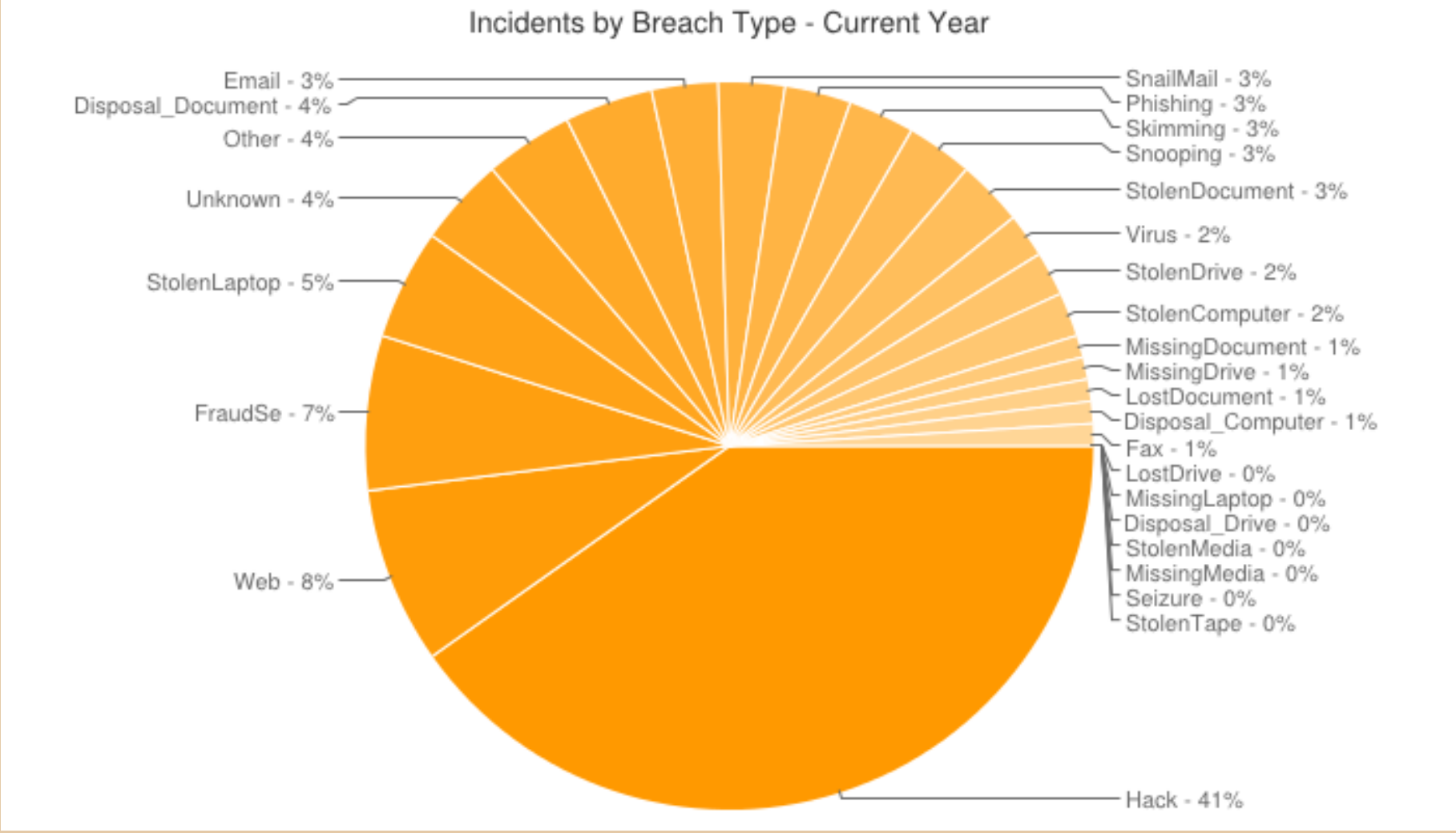
**Email: Ghahrood.A@Sarvrayaneh.com**

**Tel : +98 ( 21) 88027364 Ext.136 | Cell :+98 (912) 1964383 |**

# نمودار رخدادهای امنیتی در سالهای مختلف



# نمودار رخدادهای امنیتی بر اساس نوع نفوذ در سال ۲۰۱۴



# اهداف آموزش آگاهی های امنیتی

چه کسی مسئول امنیت است؟

هرشخص استفاده کننده از **کامپیوتر**

# اصطلاحات ضروری

**آسیب پذیری**

ضعفی در پیاده سازی و طراحی است که می تواند منجر به خطای نامطلوب در رخدادها و پیامدها شده و امنیت سیستم را به خطر بیاندازد.

**بهره برداری**

روشی برای نقض امنیت و نفوذ به سیستم IT از طریق اسیب پذیری های آن

**تهدید**

هر عمل و رخدادی که قابلیت به خطر انداختن و نقض امنیتی را داشته باشد

**سرقت اطلاعات**

هر عملی که منجر به سرقت اطلاعات افراد شود.

**حمله**

هر عملی که بطور هوشمندانه امنیت سیستم را نقض می کند.

**کرکر، هکر، نفوذکننده**

افرادی که هدف آنها نفوذ به سیستم و سرقت اطلاعات و صدمه زدن به آنها می باشد.

# خسارت های احتمالی

# مثلث امنیت


محرمانگی: نگهداری امن از داده ها.

یکپارچگی:اثبات اینکه داده ها دستکاری نشده اند.

قابلیت دسترسی: کاربران مجاز سیستم بی وقفه به اطلاعات دسترسی داشته باشند.

محدودیت امنیتی

اگر کاربر را بیشتر محدود نماییم سهولت استفاده و کارایی از بین می رود.

کارایی

سهولت استفاده

# اساس امنیت

**احتیاط**

پیروی از اقدامات پیشگیرانه همزمان با استفاده از سیستم و برنامه ها

**نگهداری**

مدیریت تمامی تغییرات برنامه ها و به روز نگه داشتن آنها

**واکنش**

اقدامات به موقع هنگام وقوع رخدادهای امنیتی

# لایه های امنیت


# چه چیزی باید امن شود؟

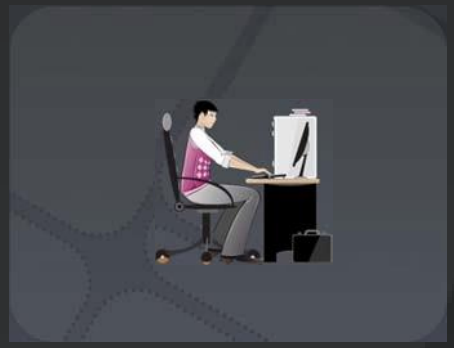
نرم افزار

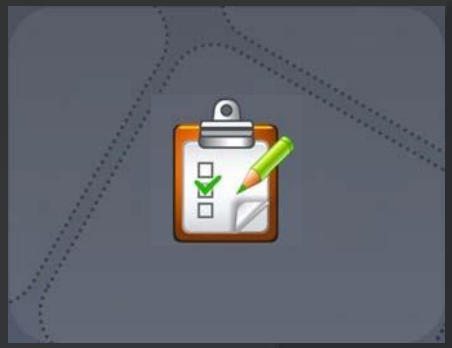
سخت افزار

ارتباطات

اطلاعات

# چه چیزهایی کامپیوتر را آسیب پذیر مینماید





# مزایای آگاهی های امنیتی

آگاهی های امنیتی باعث می شوند تا احتمال حملات کامپیوتر کاهش یابد

درجلوگیری از سرقت اطلاعات کمک می کند

به کاربران کمک می کند تا در سواستفاده  مجرمان سایبری از سیستم آنها ممانعت بعمل آورند

به کاربران کمک می کند تا در موقع بروز حادثه، خسارت را به حداقل برسانند.

به کاربران کمک می کند تا از اطلاعات حساس خود و منابع سازمان در مقابل دسترسی غیر مجاز محافظت کنند..