مدیریت امنیت سیستم‌های اطلاعاتی با رویکرد مدلسازی پویا

دکتر آمنه خدیور [*1]، خدیجه نظری ندوشن [2]

[*1] هیات علمی دانشگاه الزهرا، استادیار گروه مدیریت (گرایش مدیریت فناوری اطلاعات)

[2] کارشناس ارشد علوم کامپیوتر و دانشجوی کارشناسی ارشد MBA دانشگاه الزهرا

چکیده

مطمئنا امنیت سیستم‌های اطلاعاتی یکی از نگرانی‌های اصلی سازمان‌ها مخصوصا سازمان‌هایی است که کارشان در حیطه فناوری اطلاعات است. امنیت سیستم‌های اطلاعاتی یک مساله پیچیده است که شامل متغیرهای زیادیست و نمی توان دید خطی نسبت به آن داشت. مدلسازی پویا می تواند به عنوان یک ابزار مفید برای تحلیل روابط موجود در این زمینه مطرح شود و قادر است پیچیدگی‌های ساختاری و دینامیکی این حوزه را پوشش دهد. از میان ریسک های امنیتی، حمله‌هایی که از طریق عوامل داخلی صورت می گیرد بالاترین درصد را به خود اختصاص می دهند. از طرف دیگر این عامل کمتر در نظر گرفته می‌شود و این بی توجهی می‌تواند سازمان را دچار چالش بزرگی کند. یک کارمند ناراضی دارای انگیزه فراوان برای پایین آوردن توان سازمان است، مخصوصا اگر دسترسی او به سیستم‌های اطلاعاتی بالا باشد. در این تحقیق حمله یک کارمند داخلی به سیستم-های اطلاعاتی مورد آنالیز و بررسی قرار گرفته است و توجه بیش از اندازه مدیریت به رشد و تولید سازمان یکی از عوامل موثر در کاهش امنیت سازمان مطرح شده است.

واژگان کلیدی: *امنیت سیستم اطلاعاتی، مدلسازی پویا، عامل مخرب، کنترل های فنی امنیت*

مقدمه

وابستگی سازمان‌ها به سیستم‌های اطلاعاتی باعث شده است که امنیت این سیستم‌ها یکی از نگرانی‌های اصلی همه‌ی سازمان‌ها باشد. مدیریت اشتباه در امنیت سیستم‌های اطلاعاتی باعث می‌شود که آسیب پذیری سیستم در مقابله با حمله‌ها و مشکلات امنیتی افزایش یابد.

امنیت این سیستم‌ها یک مساله پیچیده است که شامل متغیرهای زیادیست و نمی توان دید خطی نسبت به آن داشت. مدلسازی پویا می‌تواند به عنوان یک ابزار مفید برای تحلیل روابط موجود مطرح شود و قادر است پیچیدگی‌های دینامیکی و ساختاری این حوزه را پوشش دهد.

عوامل متعددی امنیت را به خطر می‌اندازند که می توان به سه دسته کلی تکنولوژی، فرآیند و نیروی انسانی تقسیم کرد. منظور از تکنولوژی همه سخت افزارها و نرم افزارهایی هستند که سطح دسترسی افراد به اطلاعات را کنترل می‌کنند. فرآیندها نشان دهنده این هستند که شرکت چه سیاست‌ها و خط مشی‌هایی در راستای امنیت اتخاذ می‌کند و عامل انسانی به فرهنگ و تفکرات نیروی کار، بر می‌گردد که تکامل آن‌ها همراه با رشد سیستم‌های اطلاعاتی چگونه است و وفاداری آن‌ها در چه سطحی هست.

یک سازمان برای اینکه بتواند امنیت را فراهم کند باید به سه متغیر افراد، فرآیند و تکنولوژی توجه کند و در نظر نگرفتن هر کدام از این سه حوزه، امنیت سازمان را به مخاطره می اندازد. از میان متغیرهای مطرح شده کمترین توجه مدیران برای برقرای امنیت به نیروی انسانیست و این در حالیست که عامل انسانی بیشترین نقش را در تعیین میزان امنیت بر عهده دارد. در این تحقیق بت استفاده از روش مدلسازی پویا، حمله یک عامل داخلی مورد آنالیز و بررسی قرار گرفته است.

فرضیه دینامیکی

حمله داخلی زمانی اتفاق می‌افتد که عامل مخرب داخلی درمی‌یابد که سیستم اطلاعاتی شدیدا آسیب پذیر است. توجه بیش از اندازه مدیریت به عامل رشد و تولید سازمان باعث می‌شود که توجه او به امنیت کاهش یابد.

عامل مخرب برای یک حمله بزرگ بتدریج اقدام می‌کند و ابتدا اختلال‌های کوچکی در سیستم ایجاد می کند و نتایج و بازخوردهای آن از جانب مدیریت را بررسی می‌کند و اگر از جانب مدیریت واکنش جدی دریافت نکرد برای حمله اصلی آماده می‌شود.

متغیرهای اصلی مساله

technical, formal, informal

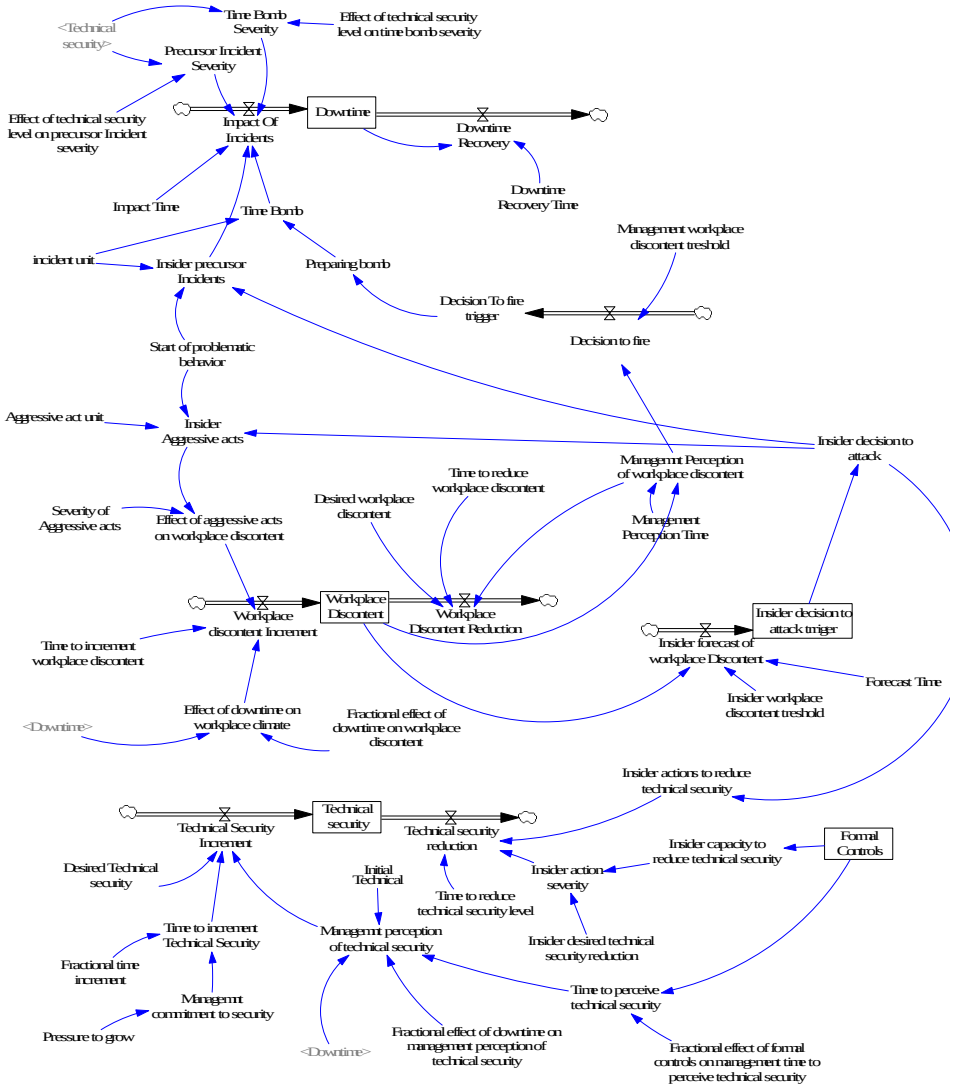
منظور از technical سخت افزارها و نرم افزارهایی است که سازمان برای حفظ امنیت سیستم‌های اطلاعاتی استفاده می‌کند. مانند آنتی ویروس‌ها، روش‌های بک آپ گیری از اطلاعات، دوربین‌های امنیتی،...

formal: این متغیر به ساختار سازمان و فرآیندهای سازمانی برمیگردد که به گونه ای هست که امنیت را برقرار کند. آگاهی‌ها و آموزش‌های استفاده کنندگان از سیستم‌های اطلاعاتی در این گروه قرار می‌گیرد.

informal: این متغیر به فرهنگ و اعتقاد نیروی کار برمی‌گردد. اینکه چقدر برای نیروی کار امنیت سازمان مهم است به مسئولیت پذیری او مربوط است و در این حیطه قرار می‌گیرد.

متغیر informal دارای تاثیر بلند مدت است و عملا اندازه گیری مستقیم نتایج آن کار دشواریست.

در شکل 1 نمودار نرخ و حالت مساله نشان داده شده است و نحوه فرمول بندی متغیرها در انتها آورده شده است.



شکل ۱- نمودار نرخ و حالت مساله

با شروع رفتار مساله ساز عامل مخرب (Start of problematic behavior)دو جریان اتفاق می‌افتد.

Insider First action, Insider aggressive acts.

این دو جریان بدون طرح و برنامه قبلی از جانب عامل ناراضی اتفاق می افتد.

جریان Insider First action مستقیما مشکلاتی را برای پایین آوردن سیستم اطلاعاتی سازمان فراهم می کند و همانطور که مشاهده می شود این تاثیر بستگی به شدت آن دارد. برای تعیین مقدار شدت مطمانا سطح متغیر Technical Security تاثیر گذار است.

در این مدل فرض شده است که متغیر Technical Security (اگر صد در صد رعایت شود) بطور کامل امنیت را در سیستم فراهم می‌کند و یا اینکه خطرهایی که سیستم را تهدید می‌کند، این خطرها قابل چشم پوشی است. بنابراین این متغیر، شدت time bomb(Time Bomb Severity) و شدت Insider First action(First action Severity) را تعیین می کند.

جریان دوم (Insider aggressive acts) شامل اقدامات کلامی یا فیزیکی است که کارمند ناراضی در ارتباط با سایر کارمندان انجام می‌دهد. این اقدامات و همچنین نابود شدن سیستم اطلاعاتی که ناشی از جریان اول بود، باعث نارضایتی سایر کارمندان می‌شود.(workplace Discontent)

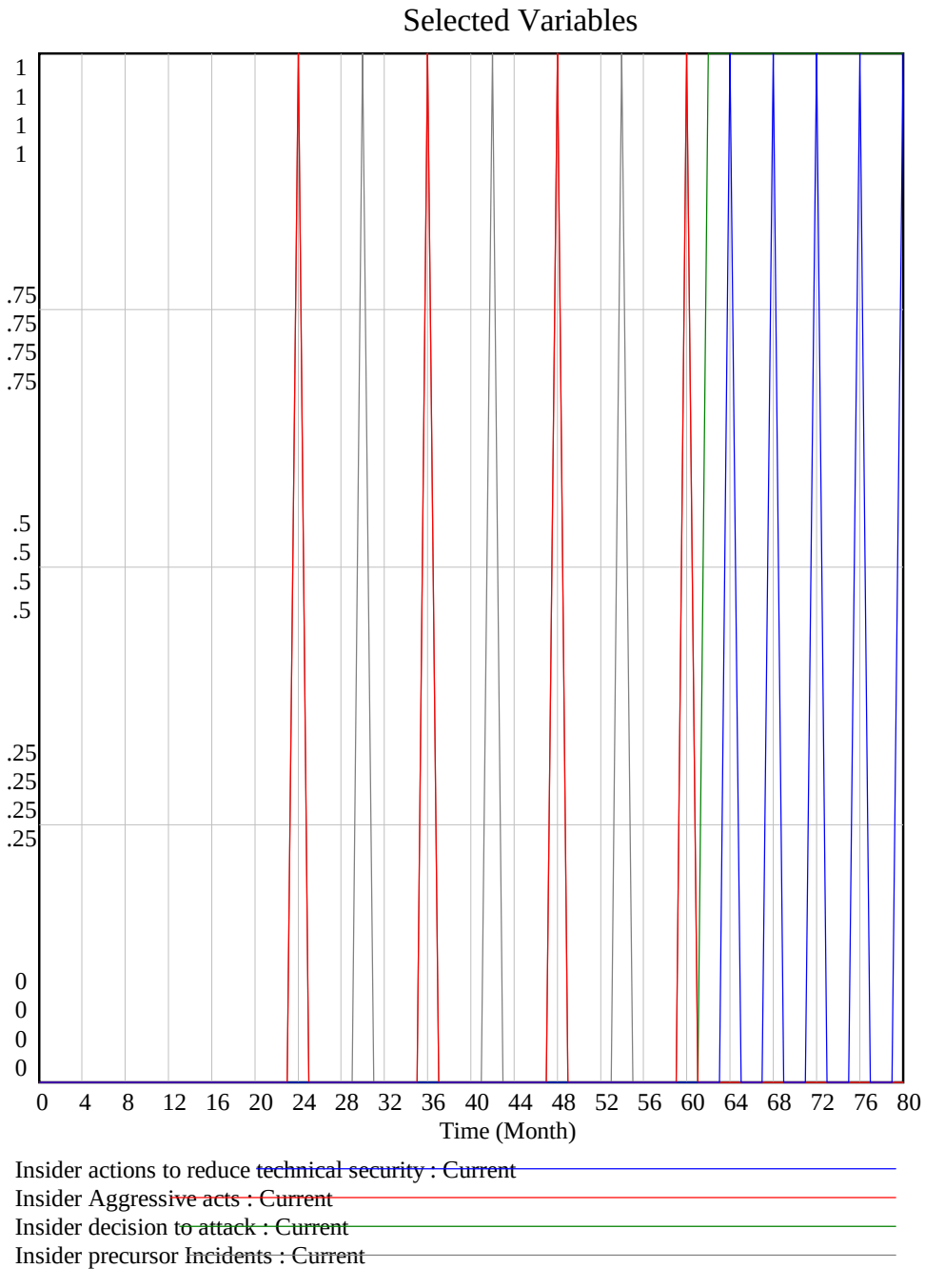
مدیر متوجه این نارضایتی محیط می شود (Management Perception Time) و به کارمند مخرب هشدار می دهد. اگر نارضایتی محیط به حد آستانه ای برسد(Insider workplace discontent threshold) مدیر تصمیم به اخراج او می‌گیرد که این باعث می شود کارمند اقدام نهایی را انجام دهد.

از طرف دیگر کارمند مخرب پیش بینی می‌کند که مدیریت تصمیم به اخراج او بگیرد(Insider forecast of workplace Discontent). براساس پیش بینی، او تصمیم به حمله می‌گیرد و اقدامات لازم را برای time bomb انجام می‌دهد. در طی زمان آماده سازی او اعمال First actions را متوقف می کند تا از جلب توجه جلوگیری کند. زمانی که مدیریت اقدام به اخراج او می‌کند او آماده اقدام نهایی است و بمب او تست شده است.

دو متغیر Management decision to fire و Insider decision to attack فقط مقدار 0و1 می گیرند.

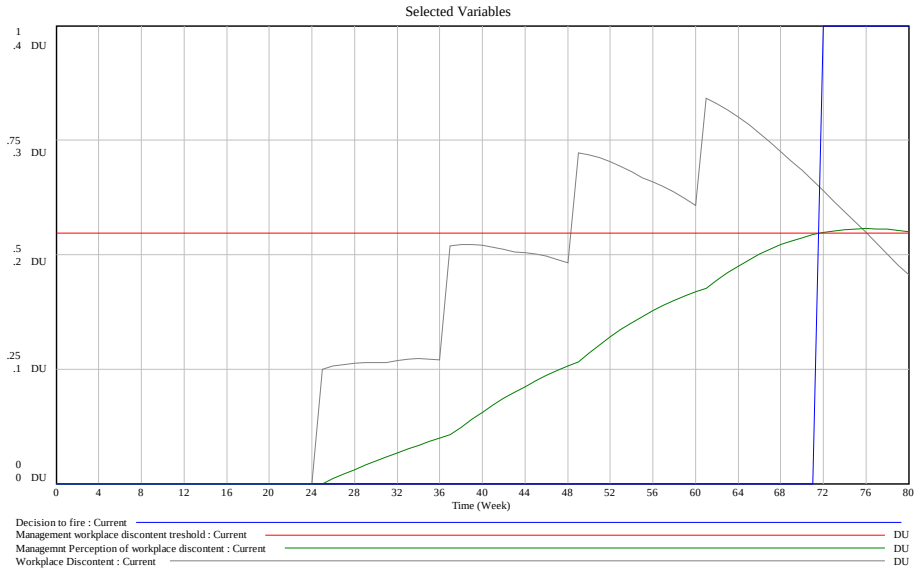
در غیاب متغیر Formal Controls متغیر Insider capacity to reduce technical security افزایش می یابد. از طرف دیگر مدیر با توجه به متغیر Formal Controls سطح امنیت سازمان را می سنجد. توجه مدیر به این متغیر و همچنین تعهد او به برقراری امنیت در سیستم (Management commitment to security) باعث افزایش technical security می‌شود(Technical Security Increment).

در شکل 2 رفتار تعدادی از متغیرها آمده است.



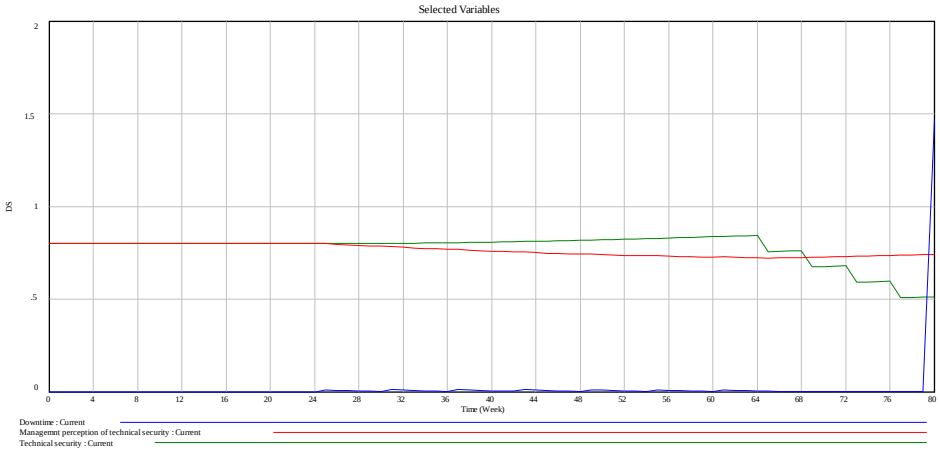
شکل 2- رفتار متغیرها

در شکل 2 مشخص است که Insider precursor Incident و Insider Aggressive acts بصورت پالس های بین 0و1 است. زمانی که عامل مخرب تصمیم به حمله می گیرد، این دو جریان متوقف می شودو Insider actions to reduce technical security شروع می شود.



شکل 3- تصمیم مدیریت برای اخراج عامل ناراضی

شکل 3 تاثیر متغیرهای Insider precursor Incident و Insider aggressive acts را روی نارضایتی محیط کار و کارمندان (Workplace Discontent) نشان می‌دهد. مدیریت این نارضایتی را احساس می کند و با حد آستانه ی خود مقایسه می‌کند. زمانی که از آن بیشتر شد(در هفته 72) مدیریت تصمیم به اخراج او می‌گیرد.

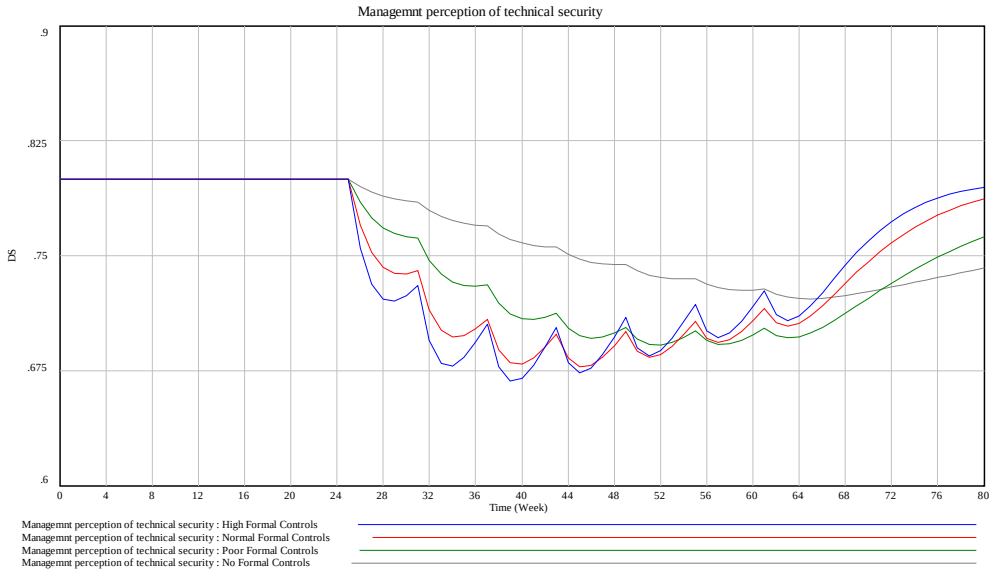


شکل 4- روند سطح امنیت سیستم اطلاعاتی

با توجه به شکل 2 در حدود هفته 60 عامل مخرب تصمیم به حمله می‌گیرد. در شکل 4 اثر این تصمیم روی کاهش Technical security دیده می‌شود. با این وجود مدیریت هنوز تهدیدی را برای امنیت احساس نمی کند. البته مدیریت، نارضایتی محیط کار را به عنوان یک عامل خطر تلقی می‌کند. در هر حال با توجه به اینکه نظارتی روی سطح امنیت در سازمان وجود ندارد، عامل مخرب همچنان موجب کاهش Technical security در سیستم می شود. و در هفته 80 سیستم نابود می شود.

سناریو

متغیر Formal Controls تاثیر مهمی روی افزایش امنیت سیستم دارد.

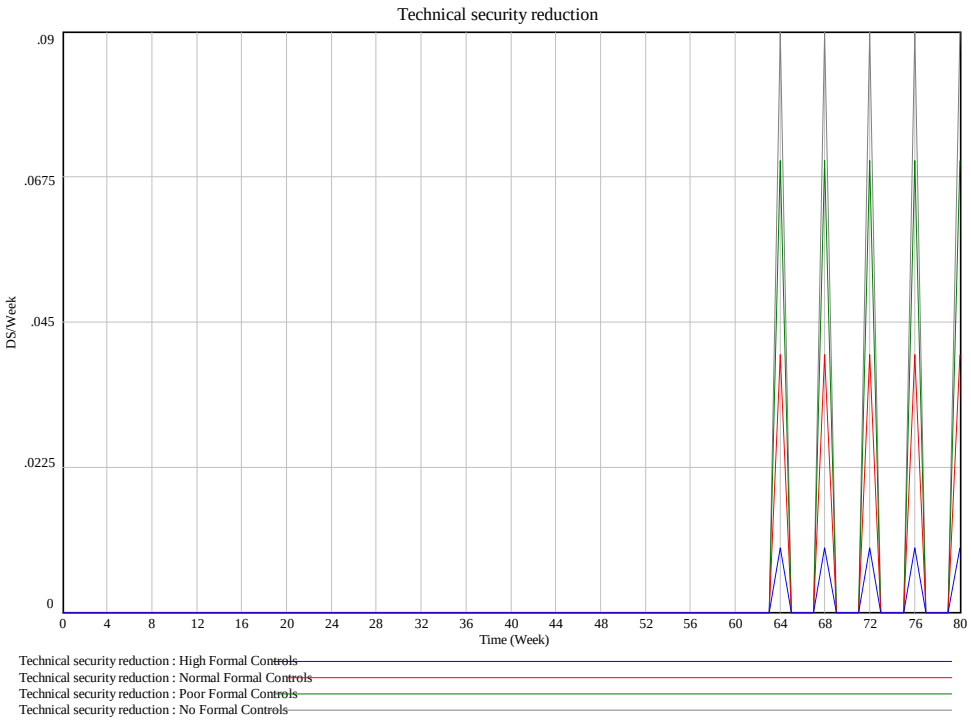


شکل 5- تاثیر متغیر formal control روی ادراک مدیریت از سطح امنیت

برای اینکه تاثیر متغیر Formal Controls را روی سایر متغیرها ببینیم مدل را به ازای مقادیر مختلف این متغیر اجرا می‌کنیم.

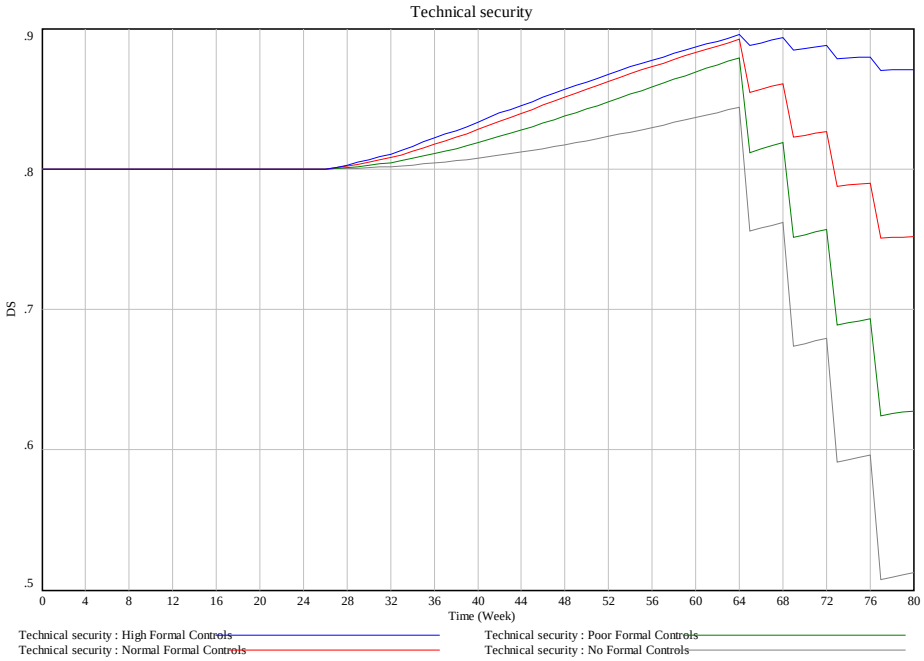
همانطور که انتظار داشتیم و در شکل 5 مشخص است با افزایش مقدار Formal Controls مقدار متغیر Management perception of technical security نیز بهبود می‌یابد و افزایش سطح متغیر Formal باعث می‌شود که درک مدیریت از Technical security و ابزارهای امنیتی سازمان افزایش یابد.

هنگامی که عامل مخرب فعالیت‌های خرابکارانه خود را شروع کرد علامت‌هایی ظاهر می‌شود و با افزایش متغیر Formal مدیریت سریع تر متوجه این علایم و کاهش امنیت سیستم می‌شود. این افزایش توجه باعث می‌شود مدیریت اقداماتی برای افزایش سطح امنیت انجام دهد.



شکل 7- تاثیر متغیر formal control بر Technical security reduction

با توجه به شکل 7 زمانی که متغیر Formal افزایش می یابد توان عامل مخرب برای خرابکاری کاهش می یابد و سطح متغیر Technical security reduction کاهش می‌یابد.

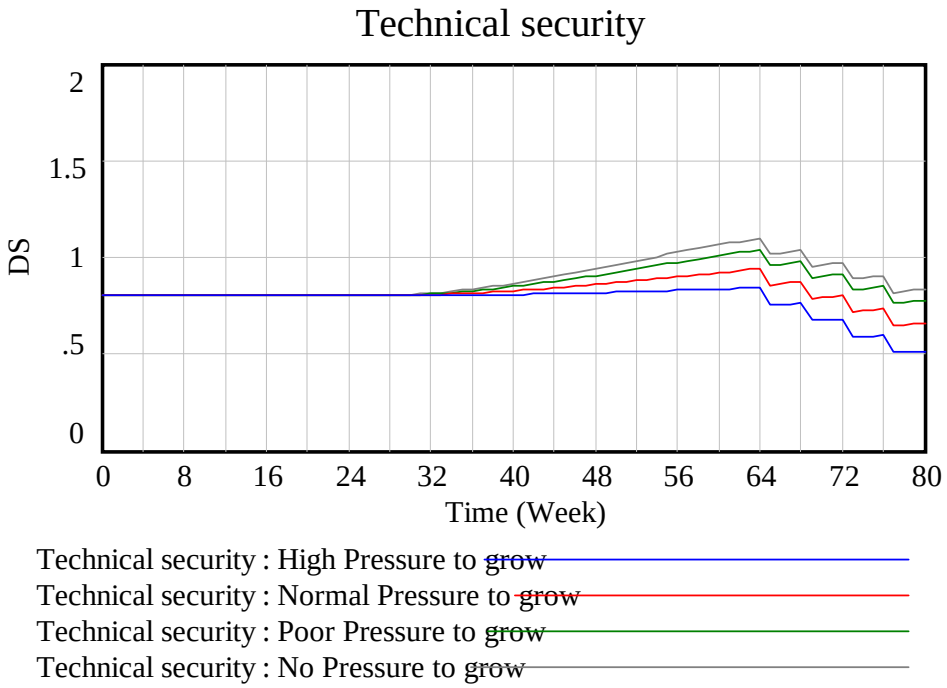


شکل 8- تاثیر متغیر formal بر امنیت سیستم اطلاعاتی

همانطور که در نمودار شکل 8 مشخص است افزایش متغیر formal باعث افزایش سطح متغیر Technical سازمان می‌شود. که این خود به دلیل افزایش درک مدیریت از وضعیت امنیتی سیستم است که قبل از اینکه اتفاق بدی روی دهد از آن جلوگیری می کند.

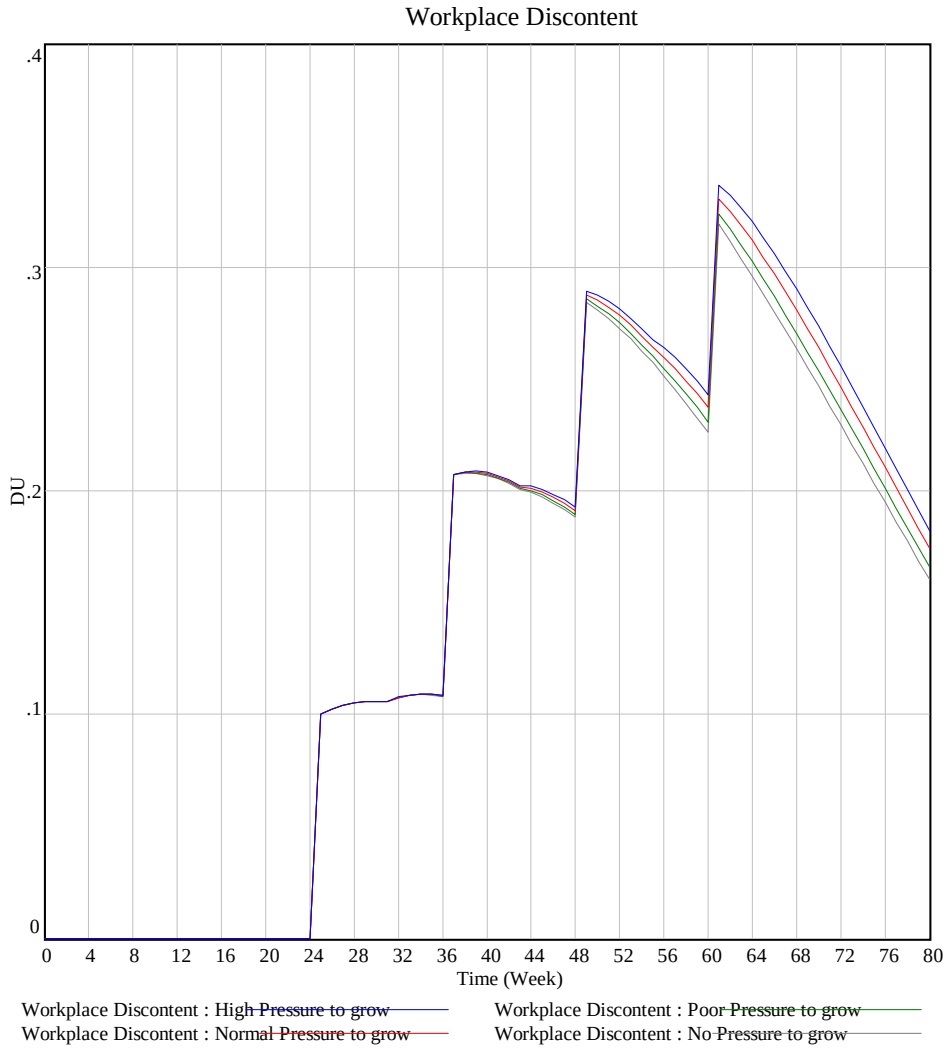
سناریوی2

با کاهش متغیر Pressure to gorw امنیت سیستم افزایش می‌یابد.



شکل 9- تاثیر متغیر Pressure to grow بر امنیت سیستم اطلاعاتی سازمان

با توجه به شکل 9 زمانی که فشار برای رشد و افزایش تولید زیاد است توجه و تعهد مدیریت برای برقراری امنیت سیستم کاهش می‌یابد و این باعث می شود سطح متغیر Technical Controls کاهش یابد و همچنین کاهش این متغیر باعث افزایش سطح نارضایتی در محیط کار (Workplace Discontent) می‌شود که در نمودار شکل 10 می‌توان مشاهده کرد.



شکل 10- تاثیر متغیر Pressure to grow بر نارضایتی محیط کار و کارمندان

نتیجه گیری

امروزه وابستگی همه سازمان‌ها به سیستم‌های اطلاعاتی امری آشکار است و توجه مدیریت به امنیت سیستم‌های اطلاعاتی برای زنده نگه داشتن سازمان حیاتیست. امنیت سیستم‌های اطلاعاتی را

می توان از سه منظر افراد، تکنولوژی و فرآیندهای سازمانی بررسی کرد. در یک سازمان بیشترین توجه مدیریت به تکنولوژی و ابزارهای فیزیکی برای برقراری امنیت است که معمولا برای جلوگیری از حمله‌های خارجیست و این در حالی است که مهم‌ترین نقش در برقراری امنیت سیستم‌های اطلاعات بر عهده افراد سازمان است. یک کارمند ناراضی دارای انگیزه کافی برای دچار مشکل کردن و حتی نابود کردن سیستم اطلاعاتی سازمان است که در این پژوهش با استفاده از مدلسازی پویا این مساله مورد بررسی قرار گرفته است.

یکی دیگر از نکاتی که در این پژوهش به آن اشاره شده است، توجه بیش از اندازه مدیریت برای رشد و بالا بردن توان تولید سازمان است که این امر نیز باعث کاهش توجه مدیریت به سیستم‌های اطلاعاتی و از طرف دیگر افزایش سطح نارضایتی کارمندان می‌شود که به تبع آن سطح امنیت سیستم‌های اطلاعاتی کاهش می‌یابد.

نحوه فرمول بندی:

Aggressive Acts Unit = 1 Action

Commitment to Security = 1 - Pressure to Grow Decision to fire = IF THEN ELSE
(Management Perception of Workplace
*Discontent>Management Workplace Discontent Threshold, 1,0) Decision to Fire Trigger = INTEG (Decision to fire, 0) Desired Technical Security = 0.8 DS Desired Workplace Discontent = 0 DU Downtime = INTEG (Impact of Incidents - Downtime Recovery, 0) DS Downtime Recovery = Downtime / Downtime Recovery Time DS/Week Downtime Recovery Time = 4 Week Effect of Aggressive Acts on Workplace Discontent = Insider Aggressive Acts **
*Severity of Aggressive Acts DU 1Effect of Downtime on Workplace Climate = Downtime * Fractional Effect of*
Downtime on Workplace Discontent DU 1Effect of Technical Security Level on Precursor Incident Severity = 0.05 1/Incident 1Effect of Technical Security Level on Time Bomb Severity = 1 1/Incident 1Forecast Time = 1 Week 1Formal Controls = 0.1 1Fractional Effect of Downtime on Management Perception of Technical Security = 2
1Fractional Effect of Downtime on Workplace Discontent = 0.5 DU/DS 1Fractional Effect of Formal Controls on Mgmt Time to Perceive Technical Security
4 Week 1

*Fractional Time Increment = 4 Week 1Impact of Incidents = (Precursor Incident Severity * Insider Precursor Incidents +*
*Time Bomb * Time Bomb Severity) / Impact Time DS/Week 2Impact Time = 1 Week 2Incidents Unit = 1 Incident 2Init TSL = 0.8 DS 2Insider Actions Severity = Insider Desired Technical Security Reduction * Insider*
Capacity to Reduce Technical Security DS/Action 2

*Insider Actions to Reduce Technical Security = Insider Decision to Attack * PULSETRAIN (0, 1, 4, 100) * Aggressive Acts Unit Action 2*
Insider Aggressive Acts = IF THEN ELSE (Start of Problematic Behavior = 1, (1 -
*Insider Decision to Attack) * PULSE TRAIN (0, 1, 12, 500), 0) * Aggressive Acts UnAction 2*
Insider Capacity to Reduce Technical Security = (1 - Formal Controls) 2Insider Decision to Attack = IF THEN ELSE (Insider Decision to Attack Trigger> =
1, 1, 0) 2Insider Decision to Attack Trigger = INTEG (Insider Forecast of Workplace
Discontent, 0) 2Insider Desired Technical Security Reduction = 0.1 DS/Action 3Insider Forecast of Workplace Discontent = IF THEN ELSE (Workplace
Discontent>Insider Workplace Discontent Threshold, 1, 0) / Forecast Time /Week 3Insider Precursor Incidents = IF THEN ELSE (Start of Problematic Behavior = 1, (
*- Insider Decision to Attack) * PULSE TRAIN (0, 1, 6, 500), 0) * Incidents Unit Incident*
*Insider Workplace Discontent Threshold = 0.3 DU 3Management Perception of Technical Security = SMOOTH (Init TSL - Downtime **
Fractional Effect of Downtime on Management Perception of Technical Security,
Time to Perceive Technical Security) DS 3
Management Perception of Workplace Discontent = SMOOTH (Workplace Discontent, Management Perception Time) DU 3
*Management Perception Time = 24 Week 3Management Workplace Discontent Threshold = 0.219DU 3Precursor Incident Severity = (1 - Technical Security Level) * Effect of Technical*
Security Level on Precursor Incident Severity DS/Incident 3Preparing Time Bomb = IF THEN ELSE (Decision to Fire Trigger>0, 1, 0) 3
Pressure to Grow = 0.9 4Severity of Aggressive Acts = 0.2 DU/Action 4Start of Problematic Behavior = STEP (1, 20) 4Technical Security Increment = (Desired Technical Security - Management
Perception of Technical Security) / Time to Increment Technical Security DS/Week 4Technical Security Level = INTEG (Technical Security Increment - Technical
*Security Reduction, Init TSL) DS 4Technical Security Reduction = Insider Actions to Reduce Technical Security **

Insider Actions Severity / Time to Reduce Technical Security Level DS/Week

Time to Increment Technical Security = Fractional Time Increment / Commitment to
Security Week
Time to Increment Workplace Discontent = 2 Week
Time to Perceive Technical Security = Fractional Effect of Formal Controls on Mgmt
Time to Perceive Technical Security / Formal Controls Week
Time to Reduce Technical Security Level = 1 Week
Time to Reduce Workplace Discontent = 24 Week
*Time Bomb = DELAY FIXED (3 * Incidents Unit * Preparing Time Bomb, 6, 0) Incident*
*Time Bomb Severity = (1 - Technical Security Level) * Effect of Technical Security*
Level on Time Bomb Severity DS/Incident
Workplace Discontent = INTEG (Workplace Discontent Increment - Workplace Discontent Reduction, 0) DU
Workplace Discontent Increment = (Effect of Aggressive Acts on Workplace Discontent + Effect of Downtime on Workplace Climate) / Time to Increment Workplace Discontent DU/Week
Workplace Discontent Reduction = (Management Perception of Workplace Discontent - Desired Workplace Discontent) / Time to Reduce Workplace Discontent

مراجع

1- Susan J. Harrington(1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *Jouranl of Management Information Systems Research Center*.
2- Andrew Simmonds, Peter Sandilands, Louis van Ekert (2007), An Ontology for Network Security Attacks. *Applied Computing.*
3- paper*information management.*
4- Behara, R, Huang, C.D, Hu, Q (2010), A system dynamics model of information security investments. *Journal of information institute publishing.*
5- DerekL.Nazareth, JaeChoi (2015), A system dynamics model for information security management. *Journal of information and management.*
6- Ross Anderson, Tyler Moore (2007), Information Security Economics – and Beyond. *Advances in Cryptology*.
7- Carl E.Landwehr (1981), Formal Models for Computer Security**.** *ACM Computing Surveys.*
8- Detmar W. Straub, Jr. and William D(1990). Nance, Discovering and Disciplining Computer Abuse in Organizations: A Field Study**.** ***MIS Quarterly.***
9- CARLOS MELARA, JOSE MARIA SARRIEGUI, JOSE J. GONZALEZ, AGATA SAWICKA, DAVID L. COOKE(2011). A System Dynamics Model of an Insider Attack on an Information System.